VMware vRealize Log Insight-Administratorhandbuch

vRealize Log Insight 3.0

Dieses Dokument unterstützt die aufgeführten Produktversionen sowie alle folgenden Versionen, bis das Dokument durch eine neue Auflage ersetzt wird. Die neuesten Versionen dieses Dokuments finden Sie unter http://www.vmware.com/de/support/pubs.

DE-001885-00

vmware®

Die neueste technische Dokumentation finden Sie auf der VMware-Website unter:

http://www.vmware.com/de/support/

Auf der VMware-Website finden Sie auch die aktuellen Produkt-Updates.

Falls Sie Anmerkungen zu dieser Dokumentation haben, senden Sie Ihre Kommentare und Vorschläge an:

docfeedback@vmware.com

Copyright © 2015 VMware, Inc. Alle Rechte vorbehalten. Informationen zu Copyright und Marken.

VMware, Inc.
3401 Hillview Ave.
Palo Alto, CA 94304
www.vmware.com

VMware Global, Inc.
Zweigniederlassung Deutschland
Freisinger Str. 3
85716 Unterschleißheim/Lohhof
Germany
Tel.: +49 (0) 89 3706 17000
Fax: +49 (0) 89 3706 17333
www.vmware.com/de

Inhalt

Informationen zum vRealize Log Insight-Administratorhandbuch 7

1 Aktualisieren von vRealize Log Insight 9
- Upgrade-Pfad für vRealize Log Insight 9
- Durchführen eines Upgrades auf vRealize Log Insight 3.0 10
- Durchführen eines Upgrades auf vRealize Log Insight 2.5 und frühere Versionen 11

2 Konfigurieren von vRealize Log Insight 15
- Grenzwerte für die Konfiguration von vRealize Log Insight 3.0 GA 16
- Konfigurieren des SSH-Root-Kennworts für die virtuelle Log Insight-Appliance 16
- Ändern der Netzwerkeinstellungen der vApp für vRealize Log Insight 17
- Zuweisen einer permanenten Lizenz zu vRealize Log Insight 18
- Protokollspeicherrichtlinie 18
- Erhöhen der Speicherkapazität der virtuellen vRealize Log Insight -Appliance 18
- Aktivieren oder Deaktivieren der Datenarchivierung in vRealize Log Insight 20
- Konfigurieren von vRealize Log Insight -Systemwarnungen 21
- Synchronisieren der Uhrzeit der virtuellen vRealize Log Insight -Appliance 28
- Konfigurieren des SMTP-Servers für vRealize Log Insight 29
- Installieren eines benutzerdefinierten SSL-Zertifikats über die vRealize Log Insight -Web-Benutzeroberfläche 30
- Ändern des Standard-Zeitlimits für vRealize Log Insight -Websitzungen 38
- Format der vRealize Log Insight -Archivdateien 38
- Importieren eines vRealize Log Insight -Archivs in vRealize Log Insight 39
- Exportieren eines Log Insight-Archivs in eine Rohtextdatei oder JSON 39
- Hinzufügen eines Ziels für die vRealize Log Insight -Ereignisweiterleitung 40
- Konfigurieren der vRealize Log Insight -Ereignisweiterleitung mit SSL 42
- Neustart des vRealize Log Insight -Diensts 42
- Ausschalten der virtuellen vRealize Log Insight -Appliance 43
- Hinzufügen von Arbeitsspeicher und CPU zur virtuellen vRealize Log Insight -Appliance 43
- Einstellen des Versands von Protokollierungsdaten an VMware 44

3 Konfigurieren von vRealize Log Insight-Clustern 45
- Hinzufügen eines Worker-Knotens zu einem vRealize Log Insight -Cluster 45
- Entfernen eines Worker-Knotens aus einem vRealize Log Insight -Cluster 49
- Aktivieren des integrierten Lastausgleichsdiensts 50

4 Konfigurieren von vRealize Log Insight-Agenten 53
- Überwachen des Status von vRealize Log Insight Windows- und Linux-Agenten 53
- Arbeiten mit Agentengruppen 54

5 Verwalten von vRealize Log Insight-Benutzerkonten 59
Benutzerverwaltung – Übersicht 59
Rollenbasierte Zugriffssteuerung 60
Erstellen eines neuen Benutzerkontos in vRealize Log Insight 60
Hinzufügen eines Active Directory-Benutzers zu vRealize Log Insight 61
Hinzufügen einer Active Directory-Gruppe zu vRealize Log Insight 62
Definieren eines Datensatzes 64
Erstellen und Ändern von Rollen 65
Löschen eines Benutzerkontos aus vRealize Log Insight 65
Aktivieren der Benutzerauthentifizierung über Active Directory 66

6 Überwachen von vRealize Log Insight 69
Prüfen des Systemzustands der virtuellen vRealize Log Insight -Appliance 69
Überwachen von Protokollereignisse sendenden Hosts 70

7 Einbinden von vRealize Log Insight in VMware-Produkte 71
Verbinden von vRealize Log Insight mit einer vSphere-Umgebung 72
Konfigurieren von vRealize Log Insight zum Senden von Benachrichtigungsereignissen an vRealize Operations Manager 79
Aktivieren der Active Directory-Integration von vRealize Log Insight und vRealize Operations Manager 81
Hinzufügen einer Suchdomäne 81
Installieren des vRealize Log Insight -Adapters in der Standalone-Version von vRealize Operations Manager 82
vRealize Operations Manager -Inhaltspaket für vRealize Log Insight 83
Aktivieren des kontextbezogenen Starts für vRealize Log Insight in vRealize Operations Manager 84
Deaktivieren des kontextbezogenen Starts für vRealize Log Insight in vRealize Operations Manager 87
Entfernen des vRealize Log Insight -Adapters aus einer vRealize Operations Manager -Instanz 88

8 Sichern, Wiederherstellen und die Notfallwiederherstellung 91
Best Practices für das Sichern, Wiederherstellen und für die Notfallwiederherstellung 91
Allgemeine Richtlinien 92
Allgemeine Empfehlungen 93
Richtlinien für das Sichern und Replizieren 93
Richtlinien für die Wiederherstellung und die Notfallwiederherstellung 95
Richtlinien für Konfigurationsänderungen nach der Wiederherstellung 96

9 Fehlerbehebung bei vRealize Log Insight 103
Es gehen keine ESXi -Protokolle mehr in vRealize Log Insight ein 103
vRealize Log Insight steht zu wenig Festplattenspeicher zur Verfügung 104
Herunterladen eines Support-Pakets für vRealize Log Insight 105
Erstellen eines Support-Pakets von vRealize Log Insight über die Virtual Appliance-Konsole 105
Zurücksetzen des Admin-Benutzerkennworts 106
Zurücksetzen des Root-Benutzerkennworts 106
Warnungen konnten nicht an vRealize Operations Manager gesendet werden 107
Anmeldung unter Verwendung der Active Directory-Anmeldedaten nicht möglich 108
SMTP funktioniert bei aktivierter STARTTLS-Option nicht 108

Fehlschlagen des Upgrades, weil die Signatur der PAK-Datei nicht validiert werden kann 109
Fehlschlagen des Upgrades mit einem internen Serverfehler 110

Index 111

Informationen zum vRealize Log Insight-Administratorhandbuch

Das *vRealize Log Insight-Administratorhandbuch* enthält Informationen zur Verwaltung von VMware® vRealize™ Log Insight™, unter anderem zur Pflege von Benutzerkonten und zur Integration von Log Insight Agents in andere VMware-Produkte. Des Weiteren enthält es Informationen zur Fehlerbehebung für Log Insight Agents.

Zielgruppe

Diese Informationen sind für Personen bestimmt, die Log Insight Agents installieren, aktualisieren oder nutzen möchten. Die Informationen sind für erfahrene Systemadministratoren bestimmt, die mit der Windows- oder Linux-VM-Technologie und Datencenteroperationen vertraut sind.

VMware Technical Publications - Glossar

VMware Technical Publications enthält ein Glossar mit Begriffen, die Ihnen möglicherweise unbekannt sind. Definitionen von Begriffen, die in der technischen Dokumentation von VMware verwendet werden, finden Sie unter http://www.vmware.com/support/pubs.

Aktualisieren von vRealize Log Insight 1

Je nach der aktuellen Version von vRealize Log Insight können Sie auf eine neuere Version aktualisieren.

Dieses Kapitel behandelt die folgenden Themen:

- „Upgrade-Pfad für vRealize Log Insight“, auf Seite 9
- „Durchführen eines Upgrades auf vRealize Log Insight 3.0“, auf Seite 10
- „Durchführen eines Upgrades auf vRealize Log Insight 2.5 und frühere Versionen“, auf Seite 11

Upgrade-Pfad für vRealize Log Insight

Der Upgrade-Pfad und -Vorgang hängt von der installierten Version von vRealize Log Insight ab, bei der Sie ein Upgrade durchführen möchten.

Installierte Version	Upgrade-Version	Upgrade-Vorgang
vRealize Log Insight 2.5 GA	vRealize Log Insight 3,0 GA	Siehe „Durchführen eines Upgrades auf vRealize Log Insight 3.0“, auf Seite 10.
vRealize Log Insight 2.5 Beta Worker-Knoten	vRealize Log Insight 2.5 GA	Siehe „Aktualisieren eines Worker-Knotens in einem vRealize Log Insight-Cluster“, auf Seite 11.
vRealize Log Insight 2.5 Beta Eigenständiger Knoten	vRealize Log Insight 2.5 GA	Siehe „Upgrade von vRealize Log Insight 1.5 GA und höher unter Verwendung der Web-Benutzeroberfläche“, auf Seite 13.
vRealize Log Insight 2.0 GA Worker-Knoten	vRealize Log Insight 2.5 Beta	Siehe „Aktualisieren eines Worker-Knotens in einem vRealize Log Insight-Cluster“, auf Seite 11.
vRealize Log Insight 2.0 GA Eigenständiger Knoten	vRealize Log Insight 2.5 Beta	Siehe „Upgrade von vRealize Log Insight 1.5 GA und höher unter Verwendung der Web-Benutzeroberfläche“, auf Seite 13.
vRealize Log Insight 2.0 Beta Worker-Knoten	vRealize Log Insight 2.0 GA	Siehe „Aktualisieren eines Worker-Knotens in einem vRealize Log Insight-Cluster“, auf Seite 11.
vRealize Log Insight 2.0 Beta eigenständig	vRealize Log Insight 2.0 GA	Siehe „Upgrade von vRealize Log Insight 1.5 GA und höher unter Verwendung der Web-Benutzeroberfläche“, auf Seite 13.

Installierte Version	Upgrade-Version	Upgrade-Vorgang
vRealize Log Insight 1.5 GA	vRealize Log Insight 2.0 GA im Clustermodus	1 „Upgrade von vRealize Log Insight 1.5 GA und höher unter Verwendung der Web-Benutzeroberfläche“, auf Seite 13. 2 „Hinzufügen eines Worker-Knotens zu einem vRealize Log Insight-Cluster“, auf Seite 45
vRealize Log Insight 1.5 GA	vRealize Log Insight 2.0 Beta	Siehe „Upgrade von vRealize Log Insight 1.5 GA und höher unter Verwendung der Web-Benutzeroberfläche“, auf Seite 13 und „Aktualisieren eines Worker-Knotens in einem vRealize Log Insight-Cluster“, auf Seite 11
vRealize Log Insight 1.5 TP2 und höher	vRealize Log Insight 1.5 GA	Weitere Informationen hierzu finden Sie unter „Upgrade von vRealize Log Insight 1.5 unter Verwendung der Web-Benutzeroberfläche“, auf Seite 13.
vRealize Log Insight 1.0 GA und 1.5 TP1	vRealize Log Insight 1.5 GA	Weitere Informationen hierzu finden Sie unter „Upgrade von vRealize Log Insight mithilfe der Befehlszeilenschnittstelle“, auf Seite 12.

Durchführen eines Upgrades auf vRealize Log Insight 3.0

Sie können bei einem Cluster automatisch ein Upgrade auf vRealize Log Insight 3.0 durchführen.

Wenn Sie den integrierten Lastausgleichsdienst verwenden, navigieren Sie zur Adresse des Lastausgleichsdiensts, anderenfalls navigieren Sie zur Adresse des Masterknotens.

Voraussetzungen

- Stellen Sie sicher, dass Sie ein Upgrade von vRealize Log Insight 2.5 GA durchführen.
- Erstellen Sie einen Snapshot oder eine Sicherungskopie der virtuellen Log Insight-Appliance.
- Fordern Sie eine Kopie des vRealize Log Insight 3.0-Upgrade-Pakets (`.pak`-Datei) an.
- Vergewissern Sie sich, dass Sie bei der Web-Benutzeroberfläche von vRealize Log Insightals Benutzer mit der Berechtigung **Admin bearbeiten** angemeldet sind. Das URL-Format lautet https://*log-insight-host*, wobei *log-insight-host* die IP-Adresse oder der Hostname der virtuellen vRealize Log Insight-Appliance ist.

Vorgehensweise

1 Klicken Sie auf das Dropdown-Menüsymbol für die Konfiguration und wählen Sie **Verwaltung** aus.

2 Klicken Sie unter „Verwaltung“ auf **Appliance**.

3 Klicken Sie auf **PAK hochladen**, um die `.pak`-Datei hochzuladen.

4 Akzeptieren Sie die neue Endbenutzer-Lizenzvereinbarung (EULA), um das Upgrade abzuschließen.

Weiter

Nach Abschluss des Masterknoten-Upgrades können Sie den verbleibenden automatischen Upgrade-Vorgang beobachten.

Achten Sie auf die an den Administrator gesendete E-Mail, die den erfolgreichen Abschluss des Upgrades bestätigt.

Durchführen eines Upgrades auf vRealize Log Insight 2.5 und frühere Versionen

Sie können ein Upgrade auf vRealize Log Insight 2.5 und frühere Versionen durchführen.

Je nach aktueller Version können Sie unter Verwendung des CLI oder über die Web-Benutzeroberfläche ein Upgrade auf vRealize Log Insight 2.x durchführen.

Aktualisieren eines Worker-Knotens in einem vRealize Log Insight -Cluster

Worker-Knoten in einem vRealize Log Insight-Cluster können aktualisiert werden.

Der vRealize Log Insight-Master-Knoten aktualisiert die Worker-Knoten zentral über die Web-Benutzeroberfläche.

Wichtig Gehen Sie beim Aktualisieren oder Hinzufügen von vRealize Log Insight-Cluster-Knoten immer der Reihe nach vor. Vermeiden Sie gleichzeitige Aktualisierungen bzw. Hinzufügungen, da dies zu Konsistenzproblemen führen kann.

Voraussetzungen

- Erstellen Sie einen Snapshot oder eine Sicherungskopie der virtuellen Log Insight-Appliance.
- Fordern Sie eine Kopie der `.pak`-Datei für das vRealize Log Insight-Upgrade-Paket an.
- Vergewissern Sie sich, dass Sie bei der Web-Benutzeroberfläche von vRealize Log Insightals Benutzer mit der Berechtigung **Admin bearbeiten** angemeldet sind. Das URL-Format lautet https://*log-insight-host*, wobei *log-insight-host* die IP-Adresse oder der Hostname der virtuellen vRealize Log Insight-Appliance ist.
- Aktualisieren Sie den Master-Knoten des vRealize Log Insight-Clusters. Weitere Informationen hierzu finden Sie unter „Upgrade von vRealize Log Insight 1.5 GA und höher unter Verwendung der Web-Benutzeroberfläche“, auf Seite 13.
- Wenn Sie einen externen Lastausgleichsdienst verwenden, nehmen Sie den Knoten aus diesem Modul heraus, bevor Sie ihn in den Wartungsmodus versetzen.

Vorgehensweise

1. Klicken Sie auf das Dropdown-Menüsymbol für die Konfiguration und wählen Sie **Verwaltung** aus.
2. Klicken Sie unter „Verwaltung“ auf **Cluster**.
3. Suchen Sie in der Tabelle „Worker“ den gewünschten Knoten und klicken Sie auf und dann auf **Weiter**.

   Der Knoten befindet sich jetzt im Wartungsmodus.

   Hinweis Ein Knoten im Wartungsmodus erhält weiterhin Protokolle.

   ---

4. Klicken Sie auf und anschließend zur Bestätigung auf **Upgrade des Workers**.

   Hinweis Das Symbol ist nur für Worker mit älteren Versionen als der Master verfügbar. Das Symbol wird nicht mehr angezeigt, nachdem der Worker auf die Version des Masters aktualisiert wurde.

   Nach dem Upgrade wird der Worker neu gestartet und neu mit dem Cluster verbunden.

Weiter

Aktualisieren Sie die übrigen Worker-Knoten in Ihrem vRealize Log Insight-Cluster.

Upgrade von vRealize Log Insight mithilfe der Befehlszeilenschnittstelle

Da vRealize Log Insight 1.0 GA und 1.5 TP1 über keine Upgrade-Benutzeroberfläche verfügen, müssen Sie eine Befehlszeilenschnittstelle verwenden, um diese Versionen auf Log Insight 1.5 zu aktualisieren.

Verwenden Sie für Upgrades der vRealize Log Insight-Versionen 1.5 TP2 und höher die Verwaltungs-Benutzeroberfläche. Weitere Informationen hierzu finden Sie unter „Upgrade von vRealize Log Insight 1.5 unter Verwendung der Web-Benutzeroberfläche“, auf Seite 13.

In diesem Vorgang wird die Konsole der virtuellen Appliance verwendet, doch können Sie ihn auch über SSH ausführen.

Hinweis Alle aktiven Benutzer der vRealize Log Insight-Instanz werden während des Aktualisierungsvorgangs abgemeldet.

Voraussetzungen

- Achten Sie darauf, in der virtuellen Log Insight-Appliance das Root-Benutzerkennwort festzulegen, um SSH- und Konsolenvorgänge zu aktivieren. Weitere Informationen hierzu finden Sie unter „Konfigurieren des SSH-Root-Kennworts für die virtuelle Log Insight-Appliance“, auf Seite 16.
- Erstellen Sie einen Snapshot oder eine Sicherungskopie der virtuellen Log Insight-Appliance.
- Fordern Sie eine Kopie der `RPM`-Datei für das vRealize Log Insight-Upgrade-Paket an.

Vorgehensweise

1. Laden Sie die `.rpm`-Datei auf einen Host mit SSH-Zugriff auf die virtuelle vRealize Log Insight-Appliance herunter.
2. Verwenden Sie das Secure Copy Protokoll, um die `.rpm`-Datei auf die virtuelle vRealize Log Insight-Appliance zu kopieren.

Betriebssystem	Kommando/Werkzeug
Linux	`scp` *`Pfad zur RPM-Datei`*`/loginsight-cloudvm-`*`version-log-insight-buildnumber`*`.x86_64.rpm root@<LogInsightIPorHostname>:~`
Windows	Laden Sie für Windows-Systeme einen SCP-Client wie WinSCP herunter.

3. Verwenden Sie die vSphere-Client-Konsole, um sich als Root-Benutzer bei der virtuellen vRealize Log Insight-Appliance anzumelden.
4. Führen Sie den Befehl `service loginsight stop` aus.
5. Führen Sie den Befehl `rpm -Uvh loginsight-cloudvm-<version>-<log-insight-build-number>.x86_64.rpm` aus und warten Sie, bis die Aktualisierung abgeschlossen ist.
6. Führen Sie den Befehl `service loginsight start` aus.
7. Stellen Sie sicher, dass Sie sich bei der Web-Benutzeroberfläche von Log Insight anmelden können.

Erinnerung Das URL-Format lautet https://log-insight-host, wobei log-insight-host die IP-Adresse oder Hostname der virtuellen vRealize Log Insight-Appliance ist.

Wenn Sie eine Fehlerseite sehen, melden Sie sich als Root-Benutzer bei der Konsole der virtuellen Appliance an und führen Sie den Befehl `service loginsight restart` aus, um den `loginsight`-Dienst neu zu starten.

Upgrade von vRealize Log Insight 1.5 unter Verwendung der Web-Benutzeroberfläche

Administratoren können vRealize Log Insight 1.5 TP2 und höher mit der Verwaltungsbenutzeroberfläche aktualisieren.

HINWEIS Alle aktiven Benutzer der vRealize Log Insight-Instanz werden während des Aktualisierungsvorgangs abgemeldet.

Voraussetzungen

- Erstellen Sie einen Snapshot oder eine Sicherungskopie der virtuellen Log Insight-Appliance.
- Fordern Sie eine Kopie der `RPM`-Datei für das vRealize Log Insight-Upgrade-Paket an.
- Vergewissern Sie sich, dass Sie bei der Web-Benutzeroberfläche von vRealize Log Insightals Benutzer mit der Berechtigung **Admin bearbeiten** angemeldet sind. Das URL-Format lautet https://*log-insight-host*, wobei *log-insight-host* die IP-Adresse oder der Hostname der virtuellen vRealize Log Insight-Appliance ist.

Vorgehensweise

1 Klicken Sie auf das Dropdown-Menüsymbol für die Konfiguration und wählen Sie **Verwaltung** aus.

2 Klicken Sie unter „Verwaltung“ auf **Appliance**.

3 Klicken Sie auf **RPM hochladen** und navigieren Sie zur `RPM`-Datei.

4 Klicken Sie auf **Upgrade durchführen**.

vRealize Log Insight lädt die `RPM`-Datei auf die virtuelle Appliance hoch und zeigt ein Bestätigungsdialogfeld an.

5 Klicken Sie zwecks Bestätigung auf **Upgrade**.

6 Akzeptieren Sie die neue Endbenutzer-Lizenzvereinbarung (EULA), um das Upgrade abzuschließen.

Upgrade von vRealize Log Insight 1.5 GA und höher unter Verwendung der Web-Benutzeroberfläche

Administratoren können vRealize Log Insight 1.5 GA und höher mit der Verwaltungsbenutzeroberfläche aktualisieren.

HINWEIS Alle aktiven Benutzer der vRealize Log Insight-Instanz werden während des Aktualisierungsvorgangs abgemeldet.

Voraussetzungen

- Erstellen Sie einen Snapshot oder eine Sicherungskopie der virtuellen Log Insight-Appliance.
- Fordern Sie eine Kopie der `.pak`-Datei für das vRealize Log Insight-Upgrade-Paket an.
- Vergewissern Sie sich, dass Sie bei der Web-Benutzeroberfläche von vRealize Log Insightals Benutzer mit der Berechtigung **Admin bearbeiten** angemeldet sind. Das URL-Format lautet https://*log-insight-host*, wobei *log-insight-host* die IP-Adresse oder der Hostname der virtuellen vRealize Log Insight-Appliance ist.

Vorgehensweise

1 Klicken Sie auf das Dropdown-Menüsymbol für die Konfiguration und wählen Sie **Verwaltung** aus.

2 Klicken Sie unter „Verwaltung“ auf **Appliance**.

3 Klicken Sie auf **PAK hochladen** und navigieren Sie zur `.pak`-Datei.

4 Klicken Sie auf **Upgrade durchführen**.

   vRealize Log Insight lädt die `.pak`-Datei zur virtuellen Appliance hoch und zeigt ein Bestätigungsdialogfeld an.

5 Klicken Sie zwecks Bestätigung auf **Upgrade**.

6 Akzeptieren Sie die neue Endbenutzer-Lizenzvereinbarung (EULA), um das Upgrade abzuschließen.

Weiter

Sie können eine neue Instanz der virtuellen vRealize Log Insight-Appliance bereitstellen und diese zum vorhandenen vRealize Log Insight-Knoten hinzufügen, um einen Cluster zu bilden. Der vorhandene Knoten wird zu einem Masterknoten und die neu bereitgestellte vRealize Log Insight-Instanz zum Worker-Knoten. Weitere Informationen hierzu finden Sie unter „Hinzufügen eines Worker-Knotens zu einem vRealize Log Insight-Cluster“, auf Seite 45.

Konfigurieren von vRealize Log Insight 2

Sie können vRealize Log Insight konfigurieren und anpassen, um Standardeinstellungen, Netzwerkeinstellungen und Speicherressourcen zu ändern. Sie können außerdem Systemwarnungen konfigurieren.

Dieses Kapitel behandelt die folgenden Themen:

- „Grenzwerte für die Konfiguration von vRealize Log Insight 3.0 GA“, auf Seite 16
- „Konfigurieren des SSH-Root-Kennworts für die virtuelle Log Insight-Appliance“, auf Seite 16
- „Ändern der Netzwerkeinstellungen der vApp für vRealize Log Insight“, auf Seite 17
- „Zuweisen einer permanenten Lizenz zu vRealize Log Insight“, auf Seite 18
- „Protokollspeicherrichtlinie“, auf Seite 18
- „Erhöhen der Speicherkapazität der virtuellen vRealize Log Insight-Appliance“, auf Seite 18
- „Aktivieren oder Deaktivieren der Datenarchivierung in vRealize Log Insight“, auf Seite 20
- „Konfigurieren von vRealize Log Insight-Systemwarnungen“, auf Seite 21
- „Synchronisieren der Uhrzeit der virtuellen vRealize Log Insight-Appliance“, auf Seite 28
- „Konfigurieren des SMTP-Servers für vRealize Log Insight“, auf Seite 29
- „Installieren eines benutzerdefinierten SSL-Zertifikats über die vRealize Log Insight-Web-Benutzeroberfläche“, auf Seite 30
- „Ändern des Standard-Zeitlimits für vRealize Log Insight-Websitzungen“, auf Seite 38
- „Format der vRealize Log Insight-Archivdateien“, auf Seite 38
- „Importieren eines vRealize Log Insight-Archivs in vRealize Log Insight“, auf Seite 39
- „Exportieren eines Log Insight-Archivs in eine Rohtextdatei oder JSON“, auf Seite 39
- „Hinzufügen eines Ziels für die vRealize Log Insight-Ereignisweiterleitung“, auf Seite 40
- „Konfigurieren der vRealize Log Insight-Ereignisweiterleitung mit SSL“, auf Seite 42
- „Neustart des vRealize Log Insight-Diensts“, auf Seite 42
- „Ausschalten der virtuellen vRealize Log Insight-Appliance“, auf Seite 43
- „Hinzufügen von Arbeitsspeicher und CPU zur virtuellen vRealize Log Insight-Appliance“, auf Seite 43
- „Einstellen des Versands von Protokollierungsdaten an VMware“, auf Seite 44

Grenzwerte für die Konfiguration von vRealize Log Insight 3.0 GA

Wenn Sie vRealize Log Insight konfigurieren, müssen Sie die Grenzwerte einhalten.

Diese Grenzwerte für die Konfiguration gelten für vRealize Log Insight 3.0 GA.

Tabelle 2-1. Maximalwerte für die Konfiguration von vRealize Log Insight 3.0 GA

Element	Maximalwert
Knoten-Konfiguration	
CPU	16 vCPUs
Arbeitsspeicher	32 GB
Speichergerät (VMDK)	2 TB - 512 Byte
Gesamter adressierbarer Speicher	4 TB (+ Betriebssystemlaufwerk)
Syslog-Verbindungen	750
Clusterkonfiguration	
Knoten	12 (Master + 11 Worker)
Aufnahme pro Knoten	
Ereignisse pro Sekunde	15.000 eps
Syslog-Nachrichtenlänge	10 KB (Textfeld)
Ingestion-API HTTP-POST-Anforderung	16 KB (Textfeld); 100 KB pro HTTP-POST-Anforderung
Windows-Ereignisprotokollkanäle	60
Integrationen	
vRealize Operations Manager	1
vSphere vCenter Server	10
Active Directory-Domäne	1
E-Mail-Server	1
DNS-Server	2
NTP-Server	4
Ereignisweiterleitungen	10

Konfigurieren des SSH-Root-Kennworts für die virtuelle Log Insight-Appliance

Die SSH-Verbindung zur virtuellen Appliance ist standardmäßig deaktiviert. Um SSH-Verbindungen zu aktivieren, müssen Sie das SSH-Root-Kennwort über VMware Remote Console konfigurieren.

Voraussetzungen

Stellen Sie sicher, dass die virtuelle vRealize Log Insight-Appliance bereitgestellt ist und ordnungsgemäß ausgeführt wird.

Vorgehensweise

1 Klicken Sie in der vSphere-Client-Bestandsliste auf die virtuelle vRealize Log Insight-Appliance und öffnen Sie die Registerkarte **Konsole**.

2 Rufen Sie mit der im Startbild angegebenen Tastenkombination eine Befehlszeile auf.

3 Geben Sie in der Konsole **root** ein und drücken Sie die Eingabetaste. Lassen Sie das Kennwort leer und drücken Sie die Eingabetaste.

   In der Konsole wird folgende Meldung angezeigt: `Kennwortänderung angefordert. Wählen Sie ein neues Kennwort.`

4 Lassen Sie das alte Kennwort leer und drücken Sie die Eingabetaste.

5 Geben Sie ein neues Kennwort für den Root-Benutzer ein, drücken Sie die Eingabetaste, geben Sie das neue Kennwort für den Root-Benutzer erneut ein und drücken Sie die Eingabetaste.

   Das Kennwort muss aus mindestens acht Zeichen bestehen und mindestens einen Großbuchstaben, einen Kleinbuchstaben, eine Ziffer und ein Sonderzeichen enthalten. Sie können dasselbe Zeichen nicht mehr als vier Mal wiederholen.

Es wird folgende Meldung angezeigt: `Kennwort geändert.`

Weiter

Sie können das Root-Kennwort verwenden, um SSH-Verbindungen zur virtuellen vRealize Log Insight-Appliance herzustellen.

Ändern der Netzwerkeinstellungen der vApp für vRealize Log Insight

Sie können die Netzwerkeinstellungen der virtuellen Appliance für vRealize Log Insight ändern, indem Sie die vApp-Eigenschaften in vSphere Client bearbeiten.

Voraussetzungen

Stellen Sie sicher, dass Sie über die erforderlichen Berechtigungen zum Bearbeiten von vApp-Eigenschaften verfügen.

Vorgehensweise

1 Schalten Sie die vRealize Log Insight-vApp aus.

2 Klicken Sie mit der rechten Maustaste auf die vRealize Log Insight-vApp in der Bestandsliste und klicken Sie auf **Einstellungen bearbeiten**.

3 Klicken Sie auf die Registerkarte **Optionen** und wählen Sie **vApp-Optionen > IP-Zuteilungsrichtlinie**.

4 Wählen Sie eine Zuteilungsoption für IP-Adressen.

Option	Beschreibung
Fest	IP-Adressen werden manuell konfiguriert. Es wird keine automatische Zuteilung vorgenommen.
Vorübergehend	IP-Adressen werden beim Einschalten der vApp automatisch mithilfe von IP-Pools aus einem angegebenen Bereich zugeteilt. Die IP-Adressen werden freigegeben, wenn die Appliance ausgeschaltet wird.
DHCP	Zum Zuteilen der IP-Adressen wird ein DHCP-Server verwendet. Die vom DHCP-Server zugewiesenen Adressen sind in den OVF-Umgebungen von virtuellen Maschinen sichtbar, die in der vApp gestartet wurden.

5 (Optional) Wenn Sie **Fest** auswählen, klicken Sie auf **vApp-Optionen > Eigenschaften** und weisen Sie der vApp für vRealize Log Insight eine IP-Adresse, eine Netzmaske, einen DNS und einen Hostnamen zu.

Vorsicht Geben Sie nicht mehr als zwei Domänennamenserver an. Wenn Sie mehr als zwei Domänennamenserver angeben, werden alle konfigurierten Domänennamenserver in der virtuellen vRealize Log Insight-Appliance ignoriert.

6 Schalten Sie die vApp für vRealize Log Insight ein.

Zuweisen einer permanenten Lizenz zu vRealize Log Insight

Sie können vRealize Log Insight nur mit einem gültigen Lizenzschlüssel nutzen.

Wenn Sie vRealize Log Insight von der VMware-Website herunterladen, erhalten Sie eine Testlizenz. Diese Lizenz ist 60 Tage lang gültig. Nach Ablauf der Testlizenz müssen Sie eine permanente Lizenz erwerben, um vRealize Log Insight weiter nutzen zu können.

Im Verwaltungsabschnitt der Web-Benutzeroberfläche von vRealize Log Insight können Sie den vRealize Log Insight-Lizenzierungsstatus überprüfen und Ihre Lizenz verwalten.

Voraussetzungen

- Beziehen Sie über My VMware™ einen gültigen Lizenzschlüssel.
- Vergewissern Sie sich, dass Sie bei der Web-Benutzeroberfläche von vRealize Log Insightals Benutzer mit der Berechtigung **Admin bearbeiten** angemeldet sind. Das URL-Format lautet https://*log-insight-host*, wobei *log-insight-host* die IP-Adresse oder der Hostname der virtuellen vRealize Log Insight-Appliance ist.

Vorgehensweise

1 Klicken Sie auf das Dropdown-Menüsymbol für die Konfiguration und wählen Sie **Verwaltung** aus.

2 Wählen Sie unter „Management“ **Lizenz**.

3 Geben Sie im Textfeld **Lizenzschlüssel** Ihren Lizenzschlüssel ein und klicken Sie auf **Schlüssel festlegen**.

4 Stellen Sie sicher, dass der Lizenzstatus „Aktiv“ ist und dass Lizenztyp und Ablauftag korrekt sind.

Protokollspeicherrichtlinie

Die virtuelle vRealize Log Insight-Appliance benötigt mindestens 100 GB Speicher für eingehende Protokolle.

Wenn das Volumen der in vRealize Log Insight importierten Protokolle die 100-GB-Grenze erreicht, werden alte Protokollmeldungen automatisch und in regelmäßigen Abständen in der Eingangsreihenfolge stillgelegt. Um alte Meldungen aufzubewahren, können Sie die Archivierungsfunktion von vRealize Log Insight aktivieren. Weitere Informationen hierzu finden Sie unter „Aktivieren oder Deaktivieren der Datenarchivierung in vRealize Log Insight“, auf Seite 20.

Von vRealize Log Insight gespeicherte Daten sind unveränderbar. Nachdem ein Protokoll importiert wurde, kann dieses erst entfernt werden, wenn es automatisch stillgelegt wird.

Erhöhen der Speicherkapazität der virtuellen vRealize Log Insight - Appliance

Sie können die Speicherressourcen, die vRealize Log Insight zugewiesen sind, erhöhen, wenn Ihre Nachfrage wächst.

Den Speicherplatz vergrößern Sie, indem Sie der virtuellen vRealize Log Insight-Appliance eine neue virtuelle Festplatte hinzufügen. Sie können so viele Festplatten hinzufügen, wie Sie benötigen und wie Ihre Umgebung zulässt.

Voraussetzungen

- Melden Sie sich bei vSphere Client als Benutzer mit Berechtigungen zum Ändern der Hardware der virtuellen Maschinen in Ihrer Umgebung an.

- Fahren Sie die virtuelle vRealize Log Insight-Appliance sicher herunter. Siehe „Ausschalten der virtuellen vRealize Log Insight-Appliance“, auf Seite 43.

Vorgehensweise

1 Klicken Sie mit der rechten Maustaste in der vSphere Client-Bestandsliste auf die virtuelle vRealize Log Insight-Maschine und wählen Sie **Einstellungen bearbeiten** aus.

2 Klicken Sie auf der Registerkarte **Hardware** auf **Hinzufügen**.

3 Wählen Sie **Festplatte**, und klicken Sie auf **Weiter**.

4 Wählen Sie **Neue virtuelle Festplatte erstellen**, und klicken Sie auf **Weiter**.

a Geben Sie die Festplattenkapazität ein.

vRealize Log Insight unterstützt virtuelle Festplatten von bis zu 2 TB. Wenn Sie mehr Kapazität benötigen, fügen Sie mehr als eine virtuelle Festplatte hinzu.

b Auswählen eines Festplattenformats.

Option	Beschreibung
Thick-Provision Lazy-Zeroed	Erstellt eine virtuelle Festplatte im Thick-Standardformat. Der für die virtuelle Festplatte erforderliche Speicherplatz wird bei Erstellung der virtuellen Festplatte zugewiesen. Die Daten, die auf dem physischen Gerät verbleiben, werden nicht während des Anlegens, sondern zu einem späteren Zeitpunkt nach dem ersten Schreibvorgang von der virtuellen Appliance gelöscht.
Thick-Provision Eager-Zeroed	Erstellt einen Typ einer virtuellen Festplatte im Thick-Format, der Clusterfunktionen, wie z. B. Fault Tolerance, unterstützt. Der Speicher, den die virtuelle Festplatte benötigt, wird beim Erstellen zugewiesen. Im Gegensatz zum Flat-Format werden die auf dem physischen Gerät verbleibenden Daten durch Nullbyte ersetzt („zeroed out“), wenn die virtuelle Festplatte erstellt wird. Das Anlegen von Festplatten in diesem Format kann wesentlich länger dauern als das Anlegen anderer Festplattentypen. Erstellen Sie, soweit möglich, die virtuelle vRealize Log Insight-Appliance mit Festplatten vom Typ Thick-Provisioned, Eager-Zeroed, um Leistung und Betrieb der virtuellen Appliance zu optimieren.
Thin Provision	Erstellt eine Festplatte im Thin-Format. Verwenden Sie dieses Format, um Speicherplatz zu sparen.

c Zum Auswählen eines Datenspeichers navigieren Sie zum Speicherort des Datenspeichers und klicken auf **Weiter**.

5 Akzeptieren Sie den Standardknoten des virtuellen Geräts und klicken Sie auf **Weiter**.

6 Überprüfen Sie die Informationen und klicken Sie auf **Beenden**.

7 Klicken Sie auf **OK**, um Ihre Änderungen zu speichern und das Dialogfeld zu schließen.

Wenn Sie die virtuelle vRealize Log Insight-Appliance hochfahren, erkennt die virtuelle Maschine die neue Festplatte und fügt sie dem Datenvolumen hinzu.

VORSICHT Nachdem Sie eine Festplatte zur virtuellen Appliance hinzugefügt haben, können Sie sie nicht mehr auf sichere Weise entfernen. Das Entfernen von Festplatten von der virtuellen vRealize Log Insight-Appliance kann zu einem vollständigen Datenverlust führen.

Aktivieren oder Deaktivieren der Datenarchivierung in vRealize Log Insight

Durch Datenarchivierung werden alte Protokolle aufbewahrt, die aus Speicherplatzgründen möglicherweise von der virtuellen vRealize Log Insight-Appliance entfernt werden könnten. vRealize Log Insight kann archivierte Daten als NFS-Mounts speichern.

vRealize Log Insight erfasst und speichert Protokolle in einer Reihe von 1-GB-Buckets auf der Festplatte. Ein Bucket besteht aus komprimierten Protokolldateien und einem Index. Es enthält alles, was zur Durchführung von Abfragen in einem bestimmten Zeitraum notwendig ist. Sobald die Größe eines Bucket 1 GB erreicht, unterbricht vRealize Log Insight die Speicherung, schließt alle Dateien und verschließt das Bucket.

Wenn die Datenarchivierung aktiviert ist, kopiert vRealize Log Insight beim Verschließen des Bucket die rohen komprimierten Protokolldateien aus dem Bucket in eine NFS-Partition. Vor der Aktivierung der Datenarchivierung verschlossene Buckets werden nachträglich nicht mehr archiviert.

Hinweis vRealize Log Insight verwaltet den für Archivierungszwecke verwendeten NFS-Mount nicht. Wenn Systembenachrichtigungen aktiviert sind, sendet vRealize Log Insight eine E-Mail, wenn der NFS-Mount bald über keinen freien Speicherplatz mehr verfügt oder nicht zur Verfügung steht. Wenn der NFS-Mount nicht genügend freien Speicherplatz hat oder länger als die Aufbewahrungszeit der virtuellen Appliance nicht verfügbar ist, stellt vRealize Log Insight die Aufnahme neuer Daten ein, bis für den NFS-Mount genügend freier Speicherplatz vorhanden ist, der NFS-Mount verfügbar oder die Archivierung deaktiviert wird.

Voraussetzungen

- Stellen Sie sicher, dass Sie Zugriff auf eine den folgenden Anforderungen entsprechende NFS-Partition haben.
  - Die NFS-Partition muss Lese- und Schreibvorgänge für Gastkonten ermöglichen.
  - Für den Mount darf keine Authentifizierung erforderlich sein.
  - Der NFS-Server muss NFS v3 unterstützen.
  - Wenn Sie einen Windows NFS-Server verwenden, aktivieren Sie die Option „Unix-Zugriff durch nicht zugeordneten Benutzer zulassen (über UID/GID)“.
- Vergewissern Sie sich, dass Sie bei der Web-Benutzeroberfläche von vRealize Log Insightals Benutzer mit der Berechtigung **Admin bearbeiten** angemeldet sind. Das URL-Format lautet https://*log-insight-host*, wobei *log-insight-host* die IP-Adresse oder der Hostname der virtuellen vRealize Log Insight-Appliance ist.

Vorgehensweise

1. Klicken Sie auf das Dropdown-Menüsymbol für die Konfiguration und wählen Sie **Verwaltung** aus.
2. Klicken Sie unter "Konfiguration"auf **Speicher**.
3. Aktivieren Sie das Kontrollkästchen **Datenarchivierung aktivieren** und geben Sie den Pfad einer NFS-Partition, auf der Protokolle archiviert werden, im Format `nfs://servername/sharename` ein.
4. Klicken Sie auf **Testverbindung**, um die Verbindung zu überprüfen.
5. Klicken Sie auf **Speichern**.

Hinweis Durch Datenarchivierung werden Protokollereignisse aufbewahrt, die aus Speicherplatzgründen von der virtuellen vRealize Log Insight-Appliance entfernt wurden. Von der virtuellen vRealize Log Insight-Appliance entfernte Protokollereignisse, die archiviert wurden, können nicht mehr durchsucht werden. Wenn Sie archivierte Protokolle durchsuchen möchten, müssen Sie diese in eine vRealize Log Insight-Instanz importieren. Weitere Informationen zum Importieren von archivierten Protokolldateien finden Sie unter „Importieren eines vRealize Log Insight-Archivs in vRealize Log Insight“, auf Seite 39.

Weiter

Stellen Sie nach dem Neustart von vRealize Log Insight sicher, dass Syslog-Feeds von ESXi nach wie vor in vRealize Log Insight ankommen. Informationen zur Fehlerbehebung finden Sie unter Es gehen keine ESXi-Protokolle mehr in Log Insight ein.

Konfigurieren von vRealize Log Insight -Systemwarnungen

Administratoren können vRealize Log Insight so konfigurieren, dass Benachrichtigungen zum eigenen Systemzustand versendet werden.

vRealize Log Insight erstellt diese Benachrichtigungen, wenn ein wichtiges Systemereignis auftritt, zum Beispiel wenn der Speicherplatz fast erschöpft ist und vRealize Log Insight alte Protokolldateien löschen oder archivieren muss.

Voraussetzungen

Vergewissern Sie sich, dass Sie bei der Web-Benutzeroberfläche von vRealize Log Insightals Benutzer mit der Berechtigung **Admin bearbeiten** angemeldet sind. Das URL-Format lautet https://*log-insight-host*, wobei *log-insight-host* die IP-Adresse oder der Hostname der virtuellen vRealize Log Insight-Appliance ist.

Vorgehensweise

1 Klicken Sie auf das Dropdown-Menüsymbol für die Konfiguration und wählen Sie **Verwaltung** aus.

2 Klicken Sie unter „Konfiguration“ auf **Allgemein**.

3 Stellen Sie unter dem Warnungs-Header die Systembenachrichtigungen ein.

   a Geben Sie im Textfeld **E-Mail-Versand von Systembenachrichtigungen an** die E-Mail-Adressen ein, an die eine Benachrichtigung gesendet werden soll.

   Trennen Sie mehrere E-Mail-Adressen durch Kommata.

   b Aktivieren Sie das Kontrollkästchen **Senden einer Benachrichtigung beim Absinken der Kapazität unter** und stellen Sie den Schwellenwert ein, der den Versand der Benachrichtigungen auslöst.

   c (Optional) Stellen Sie sicher, dass das Kontrollkästchen **Benutzerwarnungen anhalten** nicht aktiviert ist.

   Sie können dieses Kontrollkästchen aktivieren, um alle benutzerdefinierten E-Mail-Warnungen zu stoppen.

   Hinweis Systembenachrichtigungen können durch Entfernen der im Textfeld **E-Mail-Versand von Systembenachrichtigungen an** angegebenen E-Mail-Adressen deaktiviert werden (nicht empfohlen).

4 Klicken Sie auf **Speichern**.

5 Klicken Sie auf **Log Insight neu starten**, um Ihre Änderungen anzuwenden.

Übersicht über E-Mail-Benachrichtigungen und Warnungen bei vRealize Log Insight

vRealize Log Insight sendet zwei Arten von E-Mail-Benachrichtigungen: Systembenachrichtigungen und benutzerdefinierte Benachrichtigungen.

Administratoren können vRealize Log Insight so konfigurieren, dass E-Mail-Benachrichtigungen gesendet werden, wenn bestimmte Systemereignisse auftreten. Die Absenderadresse von Systembenachrichtigungs-E-Mails wird durch den Administratorbenutzer auf der SMTP-Konfigurationsseite der Verwaltungs-Benutzeroberfläche im Textfeld **Absender** konfiguriert. Weitere Informationen hierzu finden Sie unter „Konfigurieren des SMTP-Servers für vRealize Log Insight“, auf Seite 29.

Administratorbenutzer können vRealize Log Insight auch so konfigurieren, dass Benachrichtigungs-E-Mails gesendet werden, wenn die Speicherkapazität einen festgelegten Schwellenwert unterschreitet.

Jeder Benutzer von vRealize Log Insight kann Warnungsabfragen erstellen, um E-Mail-Benachrichtigungen von vRealize Log Insight zu erhalten, wenn bestimmte Kriterien erfüllt sind.

Administratorbenutzer können alle benutzerdefinierten Benachrichtigungen deaktivieren.

Typ	Warnungsname	Beschreibung
System	Älteste Daten werden bald nicht mehr durchsuchbar sein	Diese Warnung informiert Sie, wenn in vRealize Log Insight eine Stilllegung alter Daten aus dem Speicher der virtuellen Appliance bevorsteht, und gibt die bei der aktuellen Aufnahmerate erwartete Menge durchsuchbarer Daten an. Ersetzte Daten werden archiviert, wenn Sie die Archivierung konfiguriert haben, oder andernfalls gelöscht. Die Warnung wird nach jedem Neustart des vRealize Log Insight-Diensts gesendet.
System	Repository-Aufbewahrungszeit	Diese Warnung informiert Sie über die Menge der durchsuchbaren Daten, die vRealize Log Insight bei den aktuellen Aufnahmeraten auf dem in der virtuellen Appliance verfügbaren Speicherplatz speichern kann. Admin-Benutzer können den Schwellenwert für Speicherplatzmeldungen festlegen. Weitere Informationen hierzu finden Sie unter „Konfigurieren von vRealize Log Insight-Systemwarnungen“, auf Seite 21.

Typ	Warnungsname	Beschreibung
System	Verworfene Ereignisse	Diese Warnung benachrichtigt Sie darüber, dass vRealize Log Insight nicht alle eingegangenen Protokollmeldungen aufnehmen konnte. ■ Im Falle von durch den vRealize Log Insight-Server erkannten Löschungen von TCP-Meldungen wird in beiden Fällen eine Systemwarnung in folgender Weise gesendet: ■ Einmal pro Tag ■ Bei jedem manuell oder automatisch ausgeführten Neustart des vRealize Log Insight-Diensts. ■ Die E-Mail enthält die Anzahl der gelöschten Meldungen seit dem Versenden der letzten Warnungs-E-Mail und die Gesamtzahl der Meldungslöschungen seit dem letzten Neustart von vRealize Log Insight. **Hinweis** Die in der Zeile „Gesendet“ angegebene Uhrzeit wird durch den E-Mail-Client vorgegeben und ist die Zeit der lokalen Zeitzone, während im E-Mail-Text die UTC-Zeit angegeben wird.
System	Beschädigter Index-Bucket	Diese Warnung benachrichtigt Sie darüber, dass ein Teil des Festplattenindexes beschädigt ist. Ein korrupter Index weist üblicherweise auf ernsthafte Probleme im zugrunde liegenden Speichersystem hin. Der beschädigte Teil des Indexes wird von der Bedienung von Abfragen ausgeschlossen. Ein korrupter Index hat Auswirkungen auf die Aufnahme neuer Daten. vRealize Log Insight überprüft die Integrität des Indexes beim Start des Diensts. Wenn eine Beschädigung festgestellt wird, sendet vRealize Log Insight eine Systemwarnung in folgender Weise: ■ Einmal pro Tag ■ Bei jedem manuell oder automatisch ausgeführten Neustart des vRealize Log Insight-Diensts.
System	Zu wenig Speicherplatz	Diese Warnung benachrichtigt Sie darüber, dass vRealize Log Insight zu wenig zugewiesenen Speicherplatz hat. Diese Warnung deutet darauf hin, dass bei vRealize Log Insight wahrscheinlich ein mit dem Speicher in Verbindung stehendes Problem vorliegt.
System	Archivplatz bald voll	Diese Warnung benachrichtigt Sie darüber, dass der für die Archivierung von vRealize Log Insight-Daten verwendete Speicherplatz auf dem NFS-Server bald erschöpft ist.

Typ	Warnungsname	Beschreibung
System	Archivfehler	Diese Warnung benachrichtigt Sie darüber, dass ein Vorgang zur Archivierung von vRealize Log Insight-Daten auf dem NFS-Server fehlgeschlagen ist. Das bedeutet in der Regel, dass vRealize Log Insight sich nicht korrekt mit dem NFS-Server verbinden oder auf diesen schreiben kann.
System	Änderung des insgesamt bereitgestellten Festplattenspeichers	Diese Warnung benachrichtigt Sie darüber, dass sich die Gesamtgröße der Partition für die Speicherung von vRealize Log Insight-Daten verringert hat. Dies deutet in der Regel auf ein ernstes Problem im zugrunde liegenden Speichersystem hin. Wenn vRealize Log Insight diesen Umstand erkennt, wird diese Warnung in folgender Weise gesendet: ■ Sofort ■ Einmal pro Tag
System	Ausstehende Archivierungen	Diese Warnung benachrichtigt Sie darüber, dass vRealize Log Insight Daten nicht erwartungsgemäß archivieren kann. Die Warnung weist in der Regel auf Probleme mit dem von Ihnen für die Datenarchivierung konfigurierten NFS-Speicher hin.
System	Lizenz bald abgelaufen	Diese Warnung benachrichtigt Sie darüber, dass die vRealize Log Insight-Lizenz bald abläuft.
System	Lizenz ist abgelaufen	Diese Warnung benachrichtigt Sie darüber, dass die vRealize Log Insight-Lizenz abgelaufen ist.
System	Keine Verbindung mit dem AD-Server möglich	Mit dieser Warnmeldung werden Sie darüber in Kenntnis gesetzt, dass vRealize Log Insight keine Verbindung zum konfigurierten Active Directory-Server herstellen kann.

Typ	Warnungsname	Beschreibung
System	High Availability-IP-Adresse [IP-Adresse] kann nicht übernommen werden, da sie bereits von einer anderen Maschine verwendet wird	Diese Warnung besagt, dass der Log Insight-Cluster die für den integrierten Lastausgleichsdienst konfigurierte IP-Adresse nicht übernehmen konnte. Die häufigste Ursache für diese Warnung ist, dass ein anderer Host in demselben Netzwerk die IP-Adresse belegt, sodass sie nicht vom Log Insight-Cluster übernommen werden kann. Sie können diesen Konflikt lösen, indem Sie entweder die IP-Adresse auf dem Host, der sie belegt, freigeben oder den integrierten Log Insight-Lastausgleichsdienst mit einer im Netz verfügbaren statischen IP-Adresse versehen. Wenn Sie die IP-Adresse des integrierten Log Insight-Lastausgleichsdiensts ändern, müssen Sie alle Clients so konfigurieren, dass sie Protokolldaten an die neue IP-Adresse oder an einen FQDN bzw. eine URL senden, der bzw. die in diese IP-Adresse aufgelöst wird. Zudem müssen Sie von der vSphere-Integrationsseite aus die Konfiguration aller mit Log Insight integrierten vCenter Server aufheben und diese neu konfigurieren.
System	High Availability-IP-Adresse [IP-Adresse] ist aufgrund zu vieler Knotenausfälle nicht verfügbar	Diese Warnung besagt, dass die IP-Adresse für den konfigurierten integrierten Lastausgleichsdienst nicht verfügbar ist. Das bedeutet, dass Clients, die Protokolldaten an den Log Insight-Cluster über die IP-Adresse des integrierten Lastausgleichsdiensts oder einen FQDN bzw. eine URL senden, der bzw. die in diese IP-Adresse aufgelöst wird, die IP-Adresse als nicht verfügbar sehen. Die häufigste Ursache für diese Warnung ist, dass die Mehrheit der Knoten im Log Insight-Cluster nicht ordnungsgemäß arbeiten, nicht verfügbar oder vom Masterknoten aus nicht erreichbar sind. Eine weitere geläufige Ursache ist, dass die NTP-Zeitsynchronisation nicht aktiviert wurde oder es bei den konfigurierten NTP-Servern erhebliche Zeitabweichungen gibt. Sie können feststellen, ob das Problem noch besteht, indem Sie die IP-Adresse anpingen (sofern erlaubt) und prüfen, ob die Adresse nicht erreichbar ist. Sie können dieses Problem beheben, indem Sie sichergehen, dass ein Großteil der Clusterknoten ordnungsgemäß arbeitet und erreichbar ist, und die NTP-Zeitsynchronisation mit genauen NTP-Servern aktivieren.

Typ	Warnungsname	Beschreibung
System	Zu viele Migrationen der High Availability-IP-Adresse [IP-Adresse] zwischen Log Insight-Knoten	Diese Warnung besagt, dass innerhalb der letzten 10 Minuten die für den integrierten Lastausgleichsdienst konfigurierte IP-Adresse zu oft migriert wurde. Im Normalbetrieb bewegt sich die IP-Adresse nur selten zwischen Log Insight-Clusterknoten. Die IP-Adresse könnte allerdings verschoben werden, wenn der aktuelle Besitzerknoten neu gestartet oder in die Wartung versetzt wird. Der andere Grund wäre eine unzureichende Zeitsynchronisierung zwischen Log Insight-Clusterknoten, was für das ordnungsgemäße Funktionieren des Clusters unerlässlich ist. In diesem Fall können Sie das Problem beheben, indem Sie die NTP-Uhrzeitsynchronisierung mit genauen NTP-Servern ermöglichen.
Benutzerdefiniert	Warnungsabfragen	Diese Warnung benachrichtigt Sie darüber, dass die Ergebnisse einer Abfrage den Kriterien entsprechen, die Sie für die Warnung festgelegt haben. Jeder Benutzer kann Warnungsabfragen festlegen, die E-Mail-Benachrichtigungen senden, wenn bestimmte Kriterien erfüllt werden. Weitere Informationen finden Sie unter Hinzufügen einer Warnungsabfrage in Log Insight, um E-Mail-Benachrichtigungen zu senden. Weitere Informationen finden Sie im *Log Insight-Benutzerhandbuch* unter „Hinzufügen einer Warnungsabfrage in Log Insight, um E-Mail-Benachrichtigungen zu senden“.

Horizontalskalierungs-Systemwarnungen

vRealize Log Insight sendet spezifische Systemwarnungen, um Sie über Scale-Out-Ereignisse wie Knotenbeitritt und Mitgliedsstatusänderungen zu informieren.

Gesendet von	Warnungsname	Beschreibung
Master-Knoten	Genehmigung für neuen Worker-Knoten erforderlich	Diese Warnung benachrichtigt Sie über eine Mitgliedschaftsanforderung von einem Worker-Knoten. Die Anforderung muss von einem Admin-Benutzer genehmigt oder abgelehnt werden.
Master-Knoten	Neuer Worker-Knoten genehmigt	Diese Warnung benachrichtigt Sie darüber, dass ein Admin-Benutzer eine Mitgliedschaftsanforderung von einem Worker-Knoten für den Beitritt zu einem vRealize Log Insight-Cluster genehmigt hat.

Gesendet von	Warnungsname	Beschreibung
Master-Knoten	Neuer Worker-Knoten abgelehnt	Diese Warnung benachrichtigt Sie darüber, dass ein Admin-Benutzer eine Mitgliedschaftsanforderung von einem Worker-Knoten für den Beitritt zu einem vRealize Log Insight-Cluster abgelehnt hat. Sollte die Anforderung versehentlich abgelehnt worden sein, kann ein Admin-Benutzer diese über den Worker erneut ausgeben und sie anschließend im Master-Knoten genehmigen.
Master-Knoten	Maximale Anzahl unterstützter Knoten durch Worker-Knoten überschritten	Diese Warnung benachrichtigt Sie darüber, dass die maximal unterstützte Anzahl an Worker-Knoten im Log Insight-Cluster aufgrund eines neuen Worker-Knotens überschritten wurde.
Master-Knoten	Zulässige Höchstzahl an Knoten überschritten, neuer Worker-Knoten abgelehnt	Diese Warnung benachrichtigt Sie darüber, dass ein Admin-Benutzer versucht hat, dem Cluster mehr Knoten hinzuzufügen als maximal zulässig und dass der Knoten abgelehnt wurde.
Master-Knoten	Worker-Knoten getrennt	Diese Warnung benachrichtigt Sie darüber, dass ein zuvor verbundener Worker-Knoten vom vRealize Log Insight-Cluster getrennt wurde.
Master-Knoten	Worker-Knoten erneut verbunden	Diese Warnung benachrichtigt Sie darüber, dass ein Worker-Knoten wieder mit dem vRealize Log Insight-Cluster verbunden wurde.
Master-Knoten	Worker-Knoten von Admin widerrufen	Diese Warnung benachrichtigt Sie darüber, dass ein Admin-Benutzer die Mitgliedschaft eines Worker-Knotens widerrufen hat und der Knoten nicht mehr Teil des vRealize Log Insight-Clusters ist.
Master-Knoten	Unbekannter Worker-Knoten abgelehnt	Diese Warnung benachrichtigt Sie darüber, dass der vRealize Log Insight-Master-Knoten die Anforderung eines Worker-Knotens abgelehnt hat, weil der Worker-Knoten dem Master-Knoten nicht bekannt war. Handelt es sich bei dem Worker-Knoten um einen gültigen Knoten, der dem Cluster hinzugefügt werden soll, melden Sie sich beim Worker-Knoten an, entfernen Sie dessen Token-Datei und Benutzerkonfiguration unter `/storage/core/loginsight/config/` und führen Sie im Worker-Knoten `restart loginsight service` aus.

Gesendet von	Warnungsname	Beschreibung
Master-Knoten	Worker-Knoten ist in den Wartungsmodus übergegangen	Diese Warnung benachrichtigt Sie darüber, dass ein Worker-Knoten in den Wartungsmodus übergegangen ist und ein Admin-Benutzer den Wartungsmodus für den Worker-Knoten deaktivieren muss, bevor Änderungen an der Konfiguration des Worker-Knotens vorgenommen werden können und dieser Abfragen verarbeiten kann.
Master-Knoten	Worker-Knoten wieder betriebsbereit	Diese Warnung benachrichtigt Sie darüber, dass ein Worker-Knoten den Wartungsmodus verlassen hat und wieder betriebsbereit ist.
Worker-Knoten	Master ausgefallen oder vom Worker-Knoten getrennt	Diese Warnung benachrichtigt Sie darüber, dass ein Worker-Knoten, der die Warnung sendet, keinen Kontakt zum vRealize Log Insight-Master-Knoten herstellen kann. Dies könnte möglicherweise bedeuten, dass der Master-Knoten ausgefallen ist und gegebenenfalls neu gestartet werden muss. Bei einem Ausfall des Master-Knotens kann der Cluster nicht konfiguriert werden und es können keine Abfragen übermittelt werden, bis dieser wieder online ist. Worker-Knoten nehmen weiterhin Nachrichten auf. **Hinweis** Sie könnten möglicherweise viele solcher Warnungen erhalten, weil mehrere Worker-Knoten den Ausfall des Master-Knotens unabhängig voneinander registrieren und entsprechende Benachrichtigungen ausgeben könnten.
Worker-Knoten	Master-Knoten mit Worker-Knoten verbunden	Diese Warnung benachrichtigt Sie darüber, dass ein Worker-Knoten, der die Warnung sendet, wieder mit dem vRealize Log Insight-Master-Knoten verbunden ist.

Synchronisieren der Uhrzeit der virtuellen vRealize Log Insight - Appliance

Die Uhrzeit der virtuellen vRealize Log Insight-Appliance muss mit einem NTP-Server oder dem ESX-/ESXi-Host, auf dem Sie die virtuelle Appliance bereitgestellt haben, synchronisiert werden.

Die Uhrzeit ist für die Kernfunktionalität von vRealize Log Insight von entscheidender Bedeutung.

vRealize Log Insight synchronisiert standardmäßig die Uhrzeit mit einer vordefinierten Liste öffentlicher NTP-Server. Sollten öffentliche NTP-Server aufgrund einer Firewall nicht zugänglich sein, können Sie den internen NTP-Server Ihres Unternehmens nutzen. Wenn keine NTP-Server verfügbar sind, können Sie die Uhrzeit mit dem ESX-/ESXi-Host, auf dem Sie die virtuelle vRealize Log Insight-Appliance bereitgestellt haben, synchronisieren.

Voraussetzungen

Vergewissern Sie sich, dass Sie bei der Web-Benutzeroberfläche von vRealize Log Insightals Benutzer mit der Berechtigung **Admin bearbeiten** angemeldet sind. Das URL-Format lautet https://*log-insight-host*, wobei *log-insight-host* die IP-Adresse oder der Hostname der virtuellen vRealize Log Insight-Appliance ist.

Vorgehensweise

1 Klicken Sie auf das Dropdown-Menüsymbol für die Konfiguration und wählen Sie **Verwaltung** aus.

2 Klicken Sie unter „Konfiguration“ auf **Uhrzeit**.

3 Wählen Sie im Dropdown-Menü **Uhrzeit synchronisieren mit** die Zeitquelle aus.

Option	Beschreibung
NTP-Server	Synchronisiert die Uhrzeit der virtuellen vRealize Log Insight-Appliance mit der Uhrzeit eines der aufgeführten NTP-Server.
ESX/ESXi-Host	Synchronisiert die Uhrzeit der virtuellen vRealize Log Insight-Appliance mit dem ESX-/ESXi-Host, auf dem Sie die virtuelle Appliance bereitgestellt haben.

4 (Optional) Wenn Sie NTP-Server-Synchronisation ausgewählt haben, listen Sie die NTP-Server-Adressen auf und klicken Sie auf **Testen**.

Hinweis Das Testen der Verbindung zu NTP-Servern kann bis zu 20 Sekunden pro Server in Anspruch nehmen.

5 Klicken Sie auf **Speichern**.

Konfigurieren des SMTP-Servers für vRealize Log Insight

Sie können einen SMTP so konfigurieren, dass das Versenden von E-Mail-Warnungen durch vRealize Log Insight zugelassen wird.

Systemwarnungen werden erzeugt, wenn vRealize Log Insight ein wichtiges Systemereignis erkennt, zum Beispiel wenn die Speicherkapazität der virtuellen Appliance die von Ihnen festgelegten Schwellenwerte erreicht hat. Weitere Informationen hierzu finden Sie unter „Übersicht über E-Mail-Benachrichtigungen und Warnungen bei vRealize Log Insight“, auf Seite 22.

Voraussetzungen

Vergewissern Sie sich, dass Sie bei der Web-Benutzeroberfläche von vRealize Log Insightals Benutzer mit der Berechtigung **Admin bearbeiten** angemeldet sind. Das URL-Format lautet https://*log-insight-host*, wobei *log-insight-host* die IP-Adresse oder der Hostname der virtuellen vRealize Log Insight-Appliance ist.

Vorgehensweise

1 Klicken Sie auf das Dropdown-Menüsymbol für die Konfiguration und wählen Sie **Verwaltung** aus.

2 Klicken Sie unter "Konfiguration"auf **SMTP**.

3 Geben Sie die SMTP-Server-Adresse und die Portnummer ein.

4 Wenn der SMTP-Server eine verschlüsselte Verbindung verwendet, wählen Sie das Verschlüsselungsprotokoll aus.

5 Geben Sie im Textfeld **Absender** eine E-Mail-Adresse ein, die beim Versenden von Systemwarnungen verwendet werden soll.

Die **Absender**-Adresse erscheint als die Adresse des Absenders in den Systembenachrichtigungs-E-Mails. Sie muss keine echte Adresse sein und kann durch ihren Namen auf eine spezifische Instanz von vRealize Log Insight hinweisen. Beispiel: `loginsight@beispiel.com`.

6 Geben Sie einen Benutzernamen und ein Kennwort zur Authentifizierung beim SMTP-Server beim Versenden von Systemwarnungen ein.

7 Geben Sie eine Ziel-E-Mail-Adresse ein und klicken Sie auf **Test-E-Mail senden**, um die Verbindung zu überprüfen.

8 Klicken Sie auf **Speichern**.

Installieren eines benutzerdefinierten SSL-Zertifikats über die vRealize Log Insight -Web-Benutzeroberfläche

Standardmäßig installiert vRealize Log Insight ein selbstsigniertes SSL-Zertifikat auf der virtuellen Appliance.

Das selbstsignierte Zertifikat generiert Sicherheitswarnungen, wenn Sie eine Verbindung mit der vRealize Log Insight-Web-Benutzeroberfläche herstellen. Wenn Sie kein selbstsigniertes Sicherheitszertifikat verwenden möchten, können Sie ein benutzerdefiniertes SSL-Zertifikat installieren. Die einzige Funktion, die ein benutzerdefiniertes SSL-Zertifikat benötigt, ist „Ereignisweiterleitung über SSL“. Wenn Sie über ein Cluster-Setup mit ILB-Aktivierung verfügen, finden Sie unter „Aktivieren des integrierten Lastausgleichsdiensts“, auf Seite 50 die spezifischen Anforderungen für ein benutzerdefiniertes SSL-Zertifikat.

Hinweis Die vRealize Log Insight-Web-Benutzeroberfläche und das Log Insight Ingestion-Protokoll `cfapi` verwenden dasselbe Zertifikat für die Authentifizierung.

Voraussetzungen

- Stellen Sie sicher, dass Ihr benutzerdefiniertes SSL-Zertifikat die folgenden Anforderungen erfüllt.
  - Die Zertifikatsdatei enthält sowohl einen gültigen privaten Schlüssel als auch eine gültige Zertifikatskette.
  - Der privat Schlüssel wird vom RSA- oder DSA-Algorithmus generiert.
  - Der private Schlüssel ist nicht durch einen Kennwortsatz verschlüsselt.
  - Falls das Zertifikat von einer Kette anderer Zertifikate signiert wurde, sind alle anderen Zertifikate in der Zertifikatsdatei enthalten, die Sie importieren möchten.
  - Der private Schlüssel und alle Zertifikate, die in der Zertifikatsdatei enthalten sind, müssen PEM-codiert sein. vRealize Log Insight unterstützt keine DER-codierten Zertifikate und privaten Schlüssel.
  - Der private Schlüssel und alle Zertifikate, die in der Zertifikatsdatei enthalten sind, müssen im PEM-Format vorliegen. vRealize Log Insight unterstützt keine Zertifikate im Format PFX, PKCS12, PKCS7 oder anderen Formaten.
- Verketten Sie den gesamten Textkörper jedes einzelnen Zertifikats in einer einzelnen Textdatei in der folgenden Reihenfolge.
  a Privater Schlüssel: *`ihr_domänenname`*`.key`
  b Hauptzertifikat: *`ihr_domänenname`*`.crt`
  c Zwischenzertifikat: *`DigiCertCA`*`.crt`
  d Stammzertifikat: *`TrustedRoot`*`.crt`
- Die öffnenden und schließenden Tags jedes Zertifikats müssen in folgendem Format vorliegen.

```
-----BEGIN RSA PRIVATE KEY-----
(Your Private Key: your_domain_name.key)
-----END RSA PRIVATE KEY-----
-----BEGIN CERTIFICATE-----
(Your Primary SSL certificate: your_domain_name.crt)
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
(Your Intermediate certificate: DigiCertCA.crt)
```

```
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
(Your Root certificate: TrustedRoot.crt)
-----END CERTIFICATE-----
```

- Vergewissern Sie sich, dass Sie bei der Web-Benutzeroberfläche von vRealize Log Insightals Benutzer mit der Berechtigung **Admin bearbeiten** angemeldet sind. Das URL-Format lautet https://*log-insight-host*, wobei *log-insight-host* die IP-Adresse oder der Hostname der virtuellen vRealize Log Insight-Appliance ist.

Vorgehensweise

1 Generieren eines selbstsignierten Zertifikats auf Seite 31

Sie können mit dem OpenSSL-Tool ein selbstsigniertes Zertifikat für Windows oder Linux generieren.

2 Generieren einer Zertifizierungsanforderung auf Seite 32

Generieren Sie eine Zertifizierungsanforderung über das OpenSSL-Tool für Windows.

3 Anfordern einer Signatur von einer Zertifizierungsstelle auf Seite 33

Senden Sie Ihre Zertifizierungsanforderung an eine Zertifizierungsstelle Ihrer Wahl und fordern Sie eine Signatur an.

4 Verketten von Zertifikatsdateien auf Seite 33

Verknüpfen Sie Ihre Schlüssel- und Zertifikatsdateien in einer PEM-Datei.

5 Hochladen des signierten Zertifikats auf Seite 34

Sie können ein signiertes SSL-Zertifikat hochladen.

6 Konfigurieren der SSL-Verbindung zwischen dem vRealize Log Insight-Server und den Log Insight Agents auf Seite 35

Mit der SSL-Funktion können Sie über den sicheren Fluss der Ingestion-API reine SSL-Verbindungen zwischen Log Insight Agents und dem vRealize Log Insight-Server bereitstellen. Sie können zudem eine Vielzahl von SSL-Parametern von den Log Insight Agents konfigurieren.

Generieren eines selbstsignierten Zertifikats

Sie können mit dem OpenSSL-Tool ein selbstsigniertes Zertifikat für Windows oder Linux generieren.

Voraussetzungen

- Laden Sie das entsprechende Installationsprogramm für OpenSSL auf http://www.openssl.org/related/binaries.html herunter. Verwenden Sie das heruntergeladene OpenSSL-Installationsprogramm, um es auf Windows zu installieren.
- Bearbeiten Sie die Datei `openssl.cfg`, um weitere erforderliche Parameter hinzuzufügen. Stellen Sie sicher, dass der Parameter `req_extensions` im Abschnitt `[req]` definiert ist.

```
[req]
        .
        .
        req_extensions=v3_req #
```

- Fügen Sie einen adäquaten Eintrag „Alternativer Antragstellername“ für den Hostnamen oder die IP-Adresse Ihres Servers hinzu, wie beispielsweise *server-01.loginsight.domain*. Für den Hostnamen können Sie kein Muster festlegen.

  ```
  [v3_req]
          .
          .
          subjectAltName=DNS:server-01.loginsight.domain
          #subjectAltName=IP:10.27.74.215
  ```

Vorgehensweise

1 Erstellen Sie einen Ordner, in dem Ihre Zertifikatsdateien gespeichert werden sollen, zum Beispiel `C:\Certs\LI-2.6`.

2 Öffnen Sie eine Eingabeaufforderung und führen Sie den folgenden Befehl aus.

  ```
  C:\Certs\LI-2.6>openssl req -x509 -nodes -newkey 2048 -keyout server.key -out server.crt -
  days 3650
  ```

  OpenSSL fordert zur Eingabe von Zertifikatseigenschaften, einschließlich Land, Organisation usw., auf.

3 Geben Sie die IP-Adresse oder den Hostnamen Ihres vRealize Log Insight-Servers oder die vRealize Log Insight-Clusteradresse ein, wenn Lastausgleich aktiviert ist.

  Diese Eigenschaft ist die einzige, für die ein Wert angegeben werden muss.

Es werden die zwei Dateien `key.pm` und `cert.pm` erstellt.

- `key.pm` ist der PEM-kodierte private Schlüssel.
- `cert.pm` ist das selbstsignierte Zertifikat, das durch `key.pm` signiert wird.

Weiter

- Verketten Sie die Zertifikatsdateien. Weitere Informationen hierzu finden Sie unter „Verketten von Zertifikatsdateien“, auf Seite 33.
- Laden Sie das signierte Zertifikat hoch. Weitere Informationen hierzu finden Sie unter „Hochladen des signierten Zertifikats“, auf Seite 34.

Generieren einer Zertifizierungsanforderung

Generieren Sie eine Zertifizierungsanforderung über das OpenSSL-Tool für Windows.

Voraussetzungen

- Laden Sie das entsprechende Installationsprogramm für OpenSSL auf http://www.openssl.org/related/binaries.html herunter. Verwenden Sie das heruntergeladene OpenSSL-Installationsprogramm, um es auf Windows zu installieren.
- Bearbeiten Sie die Datei `openssl.cfg`, um weitere erforderliche Parameter hinzuzufügen. Stellen Sie sicher, dass der Parameter `req_extensions` im Abschnitt `[req]` definiert ist.

  ```
  [req]
          .
          .
          req_extensions=v3_req #
  ```

- Fügen Sie einen adäquaten Eintrag „Alternativer Antragstellername“ für den Hostnamen oder die IP-Adresse Ihres Servers hinzu, wie beispielsweise *server-01.loginsight.domain*. Für den Hostnamen können Sie kein Muster festlegen.

```
[v3_req]
        .
        .
subjectAltName=DNS:server-01.loginsight.domain
#subjectAltName=IP:10.27.74.215
```

Vorgehensweise

1. Erstellen Sie einen Ordner, in dem Ihre Zertifikatsdateien gespeichert werden sollen, zum Beispiel `C:\Certs\LI-2.5`.
2. Öffnen Sie eine Eingabeaufforderung und führen Sie den folgenden Befehl aus, um Ihren privaten Schlüssel zu generieren:

```
C:\Certs\LI-2.5>openssl genrsa -out server.key 2048
```

3. Erstellen Sie eine Zertifizierungsanforderung, indem Sie den folgenden Befehl ausführen:

```
C:\Certs\LI-2.5>openssl req -new -key server.key -out server.csr
```

   HINWEIS Dieser Befehl wird interaktiv ausgeführt und es werden Ihnen eine Reihe von Fragen gestellt. Ihre Antworten werden durch Ihre Zertifizierungsstelle überprüft. Ihre Antworten müssen den Angaben der mit der Eintragung Ihres Unternehmens verbundenen Rechtsdokumente entsprechen.

4. Folgen Sie den Anweisungen auf dem Bildschirm und geben Sie die Informationen ein, die in Ihren Zertifikatsantrag aufgenommen werden.

   WICHTIG Geben Sie im Feld „Common Name“ (Allgemeiner Name) den Hostnamen oder die IP-Adresse des Servers an, zum Beispiel **`mail.your.domain`**. Wenn Sie alle Subdomains einschließen möchten, geben Sie **`*your.domain`** ein.

Ihre Zertifizierungsanforderungsdatei `server.csr` wird generiert und gespeichert.

Anfordern einer Signatur von einer Zertifizierungsstelle

Senden Sie Ihre Zertifizierungsanforderung an eine Zertifizierungsstelle Ihrer Wahl und fordern Sie eine Signatur an.

Vorgehensweise

- Senden Sie Ihre `server.csr`-Datei an eine Zertifizierungsstelle.

  HINWEIS Beantragen Sie bei der Zertifizierungsstelle, Ihre Datei im PEM-Format codieren zu lassen.

  Die Zertifizierungsstelle bearbeitet Ihre Anforderung und sendet Ihnen eine im PEM-Format codierte `server.crt`-Datei zurück.

Verketten von Zertifikatsdateien

Verknüpfen Sie Ihre Schlüssel- und Zertifikatsdateien in einer PEM-Datei.

Vorgehensweise

1. Erstellen Sie eine neue `server.pem`-Datei und öffnen Sie sie in einem Texteditor.

2 Kopieren Sie den Inhalt Ihrer `server.key`-Datei und fügen Sie ihn mit dem folgenden Format in die `server.pem`-Datei ein.

```
-----BEGIN RSA PRIVATE KEY-----
(Your Private Key: server.key)
-----END RSA PRIVATE KEY-----
```

3 Kopieren Sie den Inhalt Ihrer `server.crt`-Datei und fügen Sie ihn mit dem folgenden Format in die `server.pem`-Datei ein.

```
-----BEGIN CERTIFICATE-----
  (Your Primary SSL certificate: server.crt)
-----END CERTIFICATE-----
```

4 Wenn die Zertifizierungsstellen Ihnen ein Zwischenzertifikat oder ein verkettetes Zertifikat ausgestellt haben, fügen Sie die Zwischenzertifikate oder verketteten Zertifikate im folgenden Format am Ende der öffentlichen Zertifikatsdatei an.

```
-----BEGIN RSA PRIVATE KEY-----
(Your Private Key: server.key)
-----END RSA PRIVATE KEY-----
-----BEGIN CERTIFICATE-----
(Your Primary SSL certificate: server.crt)
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
(Your Intermediate certificate: DigiCertCA.crt)
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
(Your Root certificate: TrustedRoot.crt)
-----END CERTIFICATE-----
```

5 Speichern Sie Ihre `server.pem`-Datei.

Hochladen des signierten Zertifikats

Sie können ein signiertes SSL-Zertifikat hochladen.

Vorgehensweise

1 Klicken Sie auf das Dropdown-Menüsymbol für die Konfiguration und wählen Sie **Verwaltung** aus.

2 Klicken Sie unter „Konfiguration“ auf **SSL-Zertifikat**.

3 Suchen Sie Ihr benutzerdefiniertes SSL-Zertifikat und klicken Sie auf **Öffnen**.

4 Klicken Sie auf **Speichern**.

5 Starten Sie vRealize Log Insight neu.

Weiter

Stellen Sie nach dem Neustart von vRealize Log Insight sicher, dass Syslog-Feeds von ESXi nach wie vor in vRealize Log Insight ankommen. Informationen zur Fehlerbehebung finden Sie unter Es gehen keine ESXi-Protokolle mehr in Log Insight ein.

Stellen Sie nach dem Neustart von vRealize Log Insight sicher, dass Syslog-Feeds von ESXi nach wie vor in vRealize Log Insight ankommen. Informationen zur Fehlerbehebung finden Sie im Thema über ESXi-Protokolle im *Log Insight-Administratorhandbuch*.

Konfigurieren der SSL-Verbindung zwischen dem vRealize Log Insight -Server und den Log Insight Agents

Mit der SSL-Funktion können Sie über den sicheren Fluss der Ingestion-API reine SSL-Verbindungen zwischen Log Insight Agents und dem vRealize Log Insight-Server bereitstellen. Sie können zudem eine Vielzahl von SSL-Parametern von den Log Insight Agents konfigurieren.

SSL-Hauptfunktionen

Das Verstehen der wesentlichen SSL-Funktionen kann Ihnen bei der ordnungsgemäßen Konfiguration von Log Insight Agents helfen.

Der vRealize Log Insight-Agent speichert Zertifikate und nutzt diese dann zur Verifizierung der Serveridentität bei allen Verbindungen mit einem bestimmten Server mit Ausnahme der allerersten Verbindung. Wenn sich die Serveridentität nicht bestätigen lässt, weist der vRealize Log Insight-Agent die Verbindung mit dem Server ab und vermerkt eine entsprechende Fehlermeldung im Protokoll. Die vom Agent empfangenen Zertifikate werden im Ordner `cert` gespeichert.

- Navigieren Sie unter Windows zu `C:\ProgramData\VMware\Log Insight Agent\cert`.
- Navigieren Sie unter Linux zu `/var/lib/loginsight-agent/cert`.

Wenn der vRealize Log Insight-Agent eine sichere Verbindung mit dem vRealize Log Insight-Server hergestellt hat, prüft der Agent das vom vRealize Log Insight-Server erhaltene Zertifikat auf seine Gültigkeit. Der vRealize Log Insight-Agent nutzt Stammzertifikate, denen das System vertraut.

- Der Log Insight Linux Agent lädt die vertrauenswürdigen Zertifikate von `/etc/pki/tls/certs/ca-bundle.crt` oder `/etc/ssl/certs/ca-certificates.crt`.
- Der Log Insight Windows Agent nutzt System-Stammzertifikate.

Wenn der vRealize Log Insight-Agent über ein lokal gespeichertes, selbstsigniertes Zertifikat verfügt und ein anderes gültiges, selbstsigniertes Zertifikat mit demselben öffentlichen Schlüssel empfängt, akzeptiert der Agent das neue Zertifikat. Dies kann bei der Neuerstellung eines selbstsignierten Zertifikats unter Verwendung desselben privaten Schlüssels, jedoch mit anderen Details, wie einem neuen Ablaufdatum, geschehen. Ansonsten wird die Verbindung abgewiesen.

Wenn der vRealize Log Insight-Agent über ein lokal gespeichertes, selbstsigniertes Zertifikat verfügt und ein gültiges, von einer Zertifizierungsbehörde (CA) signiertes Zertifikat empfängt, ersetzt der vRealize Log Insight-Agent stillschweigend das neue akzeptierte Zertifikat.

Wenn der vRealize Log Insight-Agent das selbstsignierte Zertifikat empfängt, nachdem er ein von einer Zertifizierungsbehörde (CA) signiertes Zertifikat erhalten hat, wird es vom Log Insight Agent zurückgewiesen. Der vRealize Log Insight-Agent akzeptiert das selbstsignierte, vom vRealize Log Insight-Server empfangene Zertifikat nur bei der ersten Verbindung mit dem Server.

Wenn der vRealize Log Insight-Agent über ein lokal gespeichertes, von einer Zertifizierungsbehörde (CA) signiertes Zertifikat verfügt und ein gültiges, von einer anderen vertrauenswürdigen Zertifizierungsbehörde (CA) signiertes Zertifikat erhält, wird dieses vom Agent zurückgewiesen. Sie können die Konfigurationsoptionen des vRealize Log Insight-Agents so modifizieren, dass dieser das neue Zertifikat annimmt. Weitere Informationen hierzu finden Sie unter „Konfigurieren der SSL-Parameter für vRealize Log Insight-Agenten“, auf Seite 36.

Erzwingen von Nur-SSL-Verbindungen

Sie können die vRealize Log Insight-Web-Benutzeroberfläche verwenden, um Log Insight Agents und die Ingestion-API so zu konfigurieren, dass nur SSL-Verbindungen mit dem Server zugelassen werden.

Hinweis Die aktuelle Version von vRealize Log Insight unterstützt keine Syslog SSL-Verbindungen und funktioniert nur für die vRealize Log Insight-Ingestion-API.

Voraussetzungen

Vergewissern Sie sich, dass Sie bei der Web-Benutzeroberfläche von vRealize Log Insightals Benutzer mit der Berechtigung **Admin bearbeiten** angemeldet sind. Das URL-Format lautet https://*log-insight-host*, wobei *log-insight-host* die IP-Adresse oder der Hostname der virtuellen vRealize Log Insight-Appliance ist.

Vorgehensweise

1 Klicken Sie auf das Dropdown-Menüsymbol für die Konfiguration und wählen Sie **Verwaltung** aus.

2 Klicken Sie unter „Konfiguration“ auf **SSL**.

3 Aktivieren Sie unter „API Server SSL“ das Kontrollkästchen **SSL-Verbindung erforderlich**.

4 Klicken Sie auf **Speichern**.

Die vRealize Log Insight-API gestattet nur SSL-Verbindungen zu dem Server. Nicht-SSL-Verbindungen werden abgewiesen.

Konfigurieren der SSL-Parameter für vRealize Log Insight -Agenten

Sie können die Konfigurationsdatei des vRealize Log Insight-Agenten bearbeiten, um die SSL-Konfiguration zu ändern, den vertrauenswürdigen Rootzertifikaten einen Pfad hinzuzufügen und festzulegen, ob Zertifikate vom Agenten akzeptiert werden.

Dieses Verfahren gilt für die vRealize Log Insight-Agenten für Windows und Linux.

Voraussetzungen

Für den Linux-Agenten von vRealize Log Insight:

- Melden Sie sich als **Root**-Benutzer an oder verwenden Sie `sudo`, um Konsolenbefehle auszuführen.
- Melden Sie sich bei dem Linux-System an, auf dem Sie den vRealize Log Insight-Linux-Agenten installiert haben. Öffnen Sie eine Konsole und führen Sie `pgrep liagent` aus, um sicherzustellen, dass der vRealize Log Insight-Linux-Agent installiert ist und ausgeführt wird.

Für den Windows-Agenten von vRealize Log Insight:

- Melden Sie sich bei dem Windows-Computer an, auf dem Sie den Windows-Agenten von vRealize Log Insight installiert haben, und starten Sie den Dienst-Manager, um zu überprüfen, ob der Agent-Dienst von VMware vRealize Log Insight installiert ist.

Vorgehensweise

1 Navigieren Sie zu dem Ordner, der die Datei `liagent.ini` enthält.

Betriebssystem	Pfad
Linux	`/var/lib/loginsight-agent/`
Windows	`%ProgramData%\VMware\Log Insight Agent`

2 Öffnen Sie die Datei `liagent.ini` in einem beliebigen Texteditor.

3 Fügen Sie dem `[server]`Abschnitt der Datei `liagent.ini` die folgenden Schlüssel hinzu.

Schlüssel	Beschreibung
`ssl_ca_path`	Der Pfad zur Bundle-Datei der vertrauenswürdigen Stammzertifikate. Wenn nicht anders festgehalten, verwendet der Windows-Agent von vRealize Log Insight System-Stammzertifikate. Der Linux-Agent von vRealize Log Insight versucht, vertrauenswürdige Zertifikate von `/etc/pki/tls/certs/ca-bundle.crt` oder `/etc/ssl/certs/ca-certificates.crt` zu laden.
`ssl_accept_any`	Legt fest, ob Zertifikate vom vRealize Log Insight-Agenten akzeptiert werden. Die möglichen Werte sind `yes`, `1`, `no` oder `0`. Wenn der Wert auf „Ja“ oder 1 festgelegt ist, akzeptiert der vRealize Log Insight-Agent jegliche Zertifikate vom Server und richtet eine sichere Verbindung zum Versenden von Daten ein. Der Standardwert lautet „Nein“. **Hinweis** Ist `ssl_accept_any` auf „Ja“ oder 1 festgelegt, akzeptiert der Log Insight-Agent Zertifikate ohne übereinstimmenden `Common Name`.
`ssl_accept_any_trusted`	Die möglichen Werte sind Ja, 1, Nein oder 0. Wenn der vRealize Log Insight-Agent über ein lokal gespeichertes, von einer vertrauenswürdigen Zertifizierungsbehörde signiertes Zertifikat verfügt und ein anderes gültiges Zertifikat empfängt, welches von einer anderen vertrauenswürdigen Zertifizierungsbehörde signiert ist, prüft er die Konfigurationsoption. Ist der Wert auf „Ja“ oder 1 festgelegt, akzeptiert der Agent das neue gültige Zertifikat. Ist der Wert auf „Nein“ oder 0 festgelegt, lehnt er das Zertifikat ab und beendet die Verbindung. Der Standardwert lautet „Nein“.
`ssl_cn`	Das selbstsignierte Zertifikat `Common Name`. Der Standardwert lautet `VMware vCenter Log Insight`. Sie können einen benutzerdefinierten `Common Name` festlegen, gegen den das Feld `Common Name` des Zertifikats geprüft werden muss. Der vRealize Log Insight-Agent überprüft das Feld `Common Name` des empfangenen Zertifikats gegen den Hostnamen, der für die Verbindung konfiguriert wurde, anhand des Schlüssels `hostname` im Bereich `[server]`. Gibt es keine Übereinstimmung, prüft der Agent das Feld `Common Name` gegen den Schlüssel `ssl_cn` in der Datei `liagent.ini`. Stimmen die Werte überein, akzeptiert der vRealize Log Insight-Agent das Zertifikat.

Hinweis Die Schlüssel werden nur verwendet, wenn das Protokoll im Bereich `[server]` auf `cfapi`festgelegt ist und wenn SSL aktiviert ist.

4 Speichern und schließen Sie die Datei `liagent.ini`.

Beispiel: Konfiguration

Es folgt ein Beispiel für eine SSL-Konfiguration.

```
proto=cfapi
port=9543
ssl=yes
ssl_ca_path=/etc/pki/tls/certs/ca-bundle.crt
ssl_accept_any=no
ssl_accept_any_trusted=yes
ssl_cn=LOGINSIGHT
```

Ändern des Standard-Zeitlimits für vRealize Log Insight - Websitzungen

Zur Gewährleistung der Sicherheit Ihrer Umgebung laufen vRealize Log Insight-Websitzungen nach 30 Minuten ab. Sie können das Zeitlimit erhöhen oder verringern.

Das Zeitlimit kann über die Web-Benutzeroberfläche geändert werden.

Voraussetzungen

Vergewissern Sie sich, dass Sie bei der Web-Benutzeroberfläche von vRealize Log Insightals Benutzer mit der Berechtigung **Admin bearbeiten** angemeldet sind. Das URL-Format lautet https://*log-insight-host*, wobei *log-insight-host* die IP-Adresse oder der Hostname der virtuellen vRealize Log Insight-Appliance ist.

Vorgehensweise

1 Klicken Sie auf das Dropdown-Menüsymbol für die Konfiguration und wählen Sie **Verwaltung** aus.

2 Klicken Sie unter „Konfiguration“ auf **Allgemein**.

3 Geben Sie im Bereich „Browsersitzung“ ein Zeitlimit in Minuten an.

Der Wert `-1` deaktiviert Sitzungszeitlimits.

4 Klicken Sie auf **Speichern**.

Format der vRealize Log Insight -Archivdateien

vRealize Log Insight archiviert Daten in einem bestimmten Format.

vRealize Log Insight speichert Archivdateien auf einem NFS-Server und organisiert diese in hierarchischen Verzeichnissen basierend auf der Archivierungszeit. Beispiel:

```
/backup/2014/08/07/16/bd234b2d-df98-44ae-991a-e0562f10a49/data.blob
```

wobei es sich bei `/backup` um den NFS-Speicherort, bei `2014/08/07/16` um den Zeitpunkt der Archivierung, bei `bd234b2d-df98-44ae-991a-e0562f10a49` um die Bucket-ID und bei `data.blob` um die archivierten Daten für das Bucket handelt.

Die Archivdaten `data.blob` bestehen aus einer komprimierten Datei, die interne vRealize Log Insight-Codierung verwendet. Sie enthält den ursprünglichen Inhalt für alle im Bucket gespeicherten Nachrichten sowie die statischen Felder wie „timestamp“ und „host“. Name, Quelle und Anwendungsname.

Sie können archivierte Daten in vRealize Log Insight importieren, archivierte Daten in eine Rohtextdatei exportieren und Nachrichteninhalt aus Archivdaten extrahieren. Siehe „Exportieren eines Log Insight-Archivs in eine Rohtextdatei oder JSON“, auf Seite 39 und „Importieren eines vRealize Log Insight-Archivs in vRealize Log Insight“, auf Seite 39.

Importieren eines vRealize Log Insight -Archivs in vRealize Log Insight

In vRealize Log Insight archivierte Protokolle können über die Befehlszeile importiert werden.

Hinweis Obwohl vRealize Log Insight historische und Echtzeitdaten gleichzeitig verarbeiten kann, empfiehlt es sich, für die Verarbeitung von importierten Protokolldateien eine separate Instanz von vRealize Log Insight einzusetzen.

Voraussetzungen

- Stellen Sie sicher, dass Sie über die Root-Benutzer-Anmeldedaten verfügen, um sich bei der virtuellen vRealize Log Insight-Appliance anzumelden.
- Stellen Sie sicher, dass Sie Zugriff auf den NFS-Server haben, auf dem die vRealize Log Insight-Protokolle archiviert werden.
- Vergewissern Sie sich, dass in der virtuellen Appliance für vRealize Log Insight genügend Speicherplatz für die importierten Protokolldateien vorhanden ist.

  Der mindestens verfügbare Speicher in der Partition `/storage/core` der virtuellen Appliance muss mindestens 10-mal so groß sein wie das archivierte Protokoll, das importiert werden soll.

Vorgehensweise

1. Stellen Sie eine SSH-Verbindung zur vRealize Log Insight-vApp her und melden Sie sich als Root-Benutzer an.
2. Stellen Sie den freigegebenen Ordner auf dem NFS-Server bereit, auf dem die archivierten Daten vorliegen.
3. Zum Importieren eines Verzeichnisses von archivierten vRealize Log Insight-Protokollen führen Sie folgenden Befehl aus.

   `/usr/lib/loginsight/application/bin/loginsight repository import` *`Path-To-Archived-Log-Data-Folder`*.

   Hinweis Der Import der archivierten Daten kann je nach Größe des Importordners sehr lange dauern.
4. Schließen Sie die SSH-Verbindung.

Weiter

Sie können die importierten Protokollereignisse durchsuchen, filtern und analysieren.

Exportieren eines Log Insight-Archivs in eine Rohtextdatei oder JSON

Über die Befehlszeile können Sie ein vRealize Log Insight-Archiv in eine gewöhnliche reine Textdatei oder in das JSON-Format exportieren.

Hinweis Dieses Verfahren richtet sich an erfahrene Benutzer. Die Befehlssyntax und Ausgabeformate können sich in späteren Versionen von vRealize Log Insight ohne Rückwärtskompatibilität ändern.

Voraussetzungen

- Stellen Sie sicher, dass Sie über die Root-Benutzer-Anmeldedaten verfügen, um sich bei der virtuellen vRealize Log Insight-Appliance anzumelden.
- Vergewissern Sie sich, dass in der virtuellen Appliance für vRealize Log Insight genügend Speicherplatz für die exportierten Dateien vorhanden ist.

Vorgehensweise

1 Stellen Sie eine SSH-Verbindung zur vRealize Log Insight-vApp her und melden Sie sich als Root-Benutzer an.

2 Erstellen Sie ein Archivverzeichnis in der vApp für vRealize Log Insight.

```
mkdir /archive
```

3 Stellen Sie den freigegebenen Ordner auf dem NFS-Server bereit, auf dem die archivierten Daten vorliegen, indem Sie folgenden Befehl ausführen.

```
mount –t nfs archive–fileshare:archive directory path /archive
```

4 Prüfen Sie den verfügbaren Speicherplatz in der vApp für vRealize Log Insight.

```
df –h
```

5 Exportieren Sie ein vRealize Log Insight-Archiv in eine reine Textdatei.

```
/usr/lib/loginsight/application/sbin/repo–exporter –d archive–file–directory output–file
```

Beispiel:

```
/usr/lib/loginsight/application/sbin/repo–exporter –d /archive/2014/08/07/16/bd234b2d–
df98–44ae–991a–e0562f10a49 /tmp/output.txt
```

6 Exportieren Sie den Inhalt einer vRealize Log Insight-Archivmeldung in das JSON-Format.

```
/usr/lib/loginsight/application/sbin/repo–exporter –F –d archive–file–directory output–file.
```

Beispiel:

```
/usr/lib/loginsight/application/sbin/repo–exporter –F –d /archive/2014/08/07/16/bd234b2d–
df98–44ae–991a–e0562f10a49 /tmp/output.json
```

7 Schließen Sie die SSH-Verbindung.

Hinzufügen eines Ziels für die vRealize Log Insight - Ereignisweiterleitung

Sie können einen vRealize Log Insight-Server so konfigurieren, dass er neben dem Speichern und Indexieren von Ereignissen eingehende Ereignisse an ein Syslog- oder Ingestion-API-Ziel weiterleitet.

Voraussetzungen

Vergewissern Sie sich, dass Sie bei der Web-Benutzeroberfläche von vRealize Log Insightals Benutzer mit der Berechtigung **Admin bearbeiten** angemeldet sind. Das URL-Format lautet https://*log-insight-host*, wobei *log-insight-host* die IP-Adresse oder der Hostname der virtuellen vRealize Log Insight-Appliance ist.

Stellen Sie sicher, dass das Ziel die Anzahl der weitergeleiteten Ereignisse verarbeiten kann. Wenn das Zielcluster viel kleiner als die Weiterleitungsinstanz ist, werden manche Ereignisse eventuell gelöscht.

Vorgehensweise

1 Klicken Sie auf das Dropdown-Menüsymbol für die Konfiguration und wählen Sie **Verwaltung** aus.

2 Klicken Sie unter „Verwaltung“ auf **Ereignisweiterleitung**.

3 Klicken Sie auf **Neues Ziel** und geben Sie die erforderlichen Informationen ein.

Option	Beschreibung
Name	Der eindeutige Name des neuen Ziels
Host	Die IP-Adresse oder der vollständig qualifizierte Domänenname **Vorsicht** Beim Konfigurieren von Weiterleitungszielen ist die Eingabe von IP-Adressen und Hostnamen für den Master, den Knoten und den integrierten Lastausgleichsdienst eingeschränkt. Achten Sie darauf, dass Sie keine Netzwerkschleifen generieren, die Probleme bei der Funktionalität hervorrufen können, wie z. B. das Melden von doppelten Ereignissen.
Protokoll	Ingestion-API oder Syslog. Die Standardeinstellung ist Ingestion-API. Wenn Ereignisse mithilfe der Ingestion-API weitergeleitet werden, wird die ursprüngliche Quelle des Ereignisses im Quellfeld aufbewahrt. Wenn Ereignisse mithilfe von Syslog weitergeleitet werden, geht die ursprüngliche Quelle des Ereignisses verloren und der Empfänger nimmt die Quelle der Nachricht als IP-Adresse oder Hostname der vRealize Log Insight-Ereignisweiterleitung auf.

4 (Optional) Fügen Sie Tags hinzu.

Mit Tags können Sie Ereignissen Felder mit vordefinierten Werten hinzufügen, um die Abfragen zu vereinfachen. Sie können mehrere durch Kommas getrennte Tags hinzufügen.

Hinweis Tags sind nur im Zusammenhang mit der Ingestion-API verfügbar.

5 (Optional) Um die weitergeleiteten Ereignisse einzuschränken, klicken Sie auf **Filter hinzufügen**.

Wenn Sie keinen Filter auswählen, werden alle Ereignisse weitergeleitet.

6 (Optional) Klicken Sie auf **Erweiterte Einstellungen anzeigen**, um die folgenden Weiterleitungseinstellungen zu ändern.

Option	Beschreibung
Port	Der Port, an den die Ereignisse im Remoteziel gesendet werden. Die Standardeinstellung wird anhand des angegebenen Protokolls festgelegt. Ändern Sie sie nur, wenn das Remoteziel einen anderen Port überwacht.
Festplatten-Cache	Die Menge an lokalem Festplattenspeicher, die zur Zwischenspeicherung der weiterzuleitenden Ereignisse reserviert wird. Die Zwischenspeicherung wird verwendet, wenn das Remoteziel nicht verfügbar ist oder die empfangenen Ereignisse nicht verarbeiten kann. Wenn der lokale Pufferspeicher voll und das Remoteziel noch nicht verfügbar ist, werden die ältesten lokalen Ereignisse gelöscht und nicht an das Remoteziel weitergeleitet, selbst wenn das Remoteziel wieder online ist. Die Standardeinstellung ist 200 MB.
Anzahl Worker	Die verwendete Anzahl gleichzeitiger ausgehender Verbindungen. Geben Sie eine höhere Anzahl von Workern an, um eine höhere Netzwerklatenz zum weitergeleiteten Ziel zu erreichen und mehr Ereignisse pro Sekunde weiterzuleiten. Die Standardeinstellung ist 2.

7 Klicken Sie zum Prüfen Ihrer Konfiguration auf **Test**.

8 Klicken Sie auf **Speichern**.

Weiter

- „Konfigurieren der vRealize Log Insight-Ereignisweiterleitung mit SSL“, auf Seite 42.
- Ereignisweiterleitungsziele können bearbeitet oder geklont werden.

Konfigurieren der vRealize Log Insight -Ereignisweiterleitung mit SSL

Sie können einen vRealize Log Insight-Server auf die Weiterleitung eingehender Ereignisse an ein Syslog- oder Ingestion-API-Ziel mit SSL konfigurieren.

Voraussetzungen

Die Ereignisweiterleitung mit SSL funktioniert nicht mit dem selbstsignierten Zertifikat, das standardmäßig auf den Zielservern installiert ist. Ein benutzerdefiniertes SSL-Zertifikat muss anhand der unter „Generieren einer Zertifizierungsanforderung“, auf Seite 32 aufgeführten Schritte erstellt und anschließend hochgeladen werden. Siehe „Installieren eines benutzerdefinierten SSL-Zertifikats über die vRealize Log Insight-Web-Benutzeroberfläche“, auf Seite 30.

Vorgehensweise

1 Kopieren Sie das vertrauenswürdige Stammzertifikat in ein temporäres Verzeichnis auf der Weiterleitungsinstanz. Beispiel: `/home`.

2 SSH an die Weiterleitungsinstanz, und führen Sie die folgenden Befehle aus.

```
localhost:~ # cd /usr/java/jre1.7.0_51/lib/security/
localhost:/usr/java/jre1.7.0_51/lib/security # ../../bin/keytool
–import –alias loginsight –file /home/cacert.crt –keystore cacerts
```

Das Standard-Keystore-Kennwort ist **`changeit`**.

Hinweis Java-Versionen können mit der Zeit variieren.

3 Starten Sie die vRealize Log Insight-Instanz neu.

Weiter

Aktivieren Sie die SSL-Verbindung. Weitere Informationen hierzu finden Sie unter „Erzwingen von Nur-SSL-Verbindungen“, auf Seite 35.

Neustart des vRealize Log Insight -Diensts

Sie können vRealize Log Insight über die Verwaltungsseite der Web-Benutzeroberfläche neu starten.

Vorsicht Bei einem Neustart von vRealize Log Insight werden alle aktiven Benutzersitzungen geschlossen. Benutzer der vRealize Log Insight-Instanz müssen sich erneut anmelden.

Voraussetzungen

Vergewissern Sie sich, dass Sie bei der Web-Benutzeroberfläche von vRealize Log Insightals Benutzer mit der Berechtigung **Admin bearbeiten** angemeldet sind. Das URL-Format lautet https://*log-insight-host*, wobei *log-insight-host* die IP-Adresse oder der Hostname der virtuellen vRealize Log Insight-Appliance ist.

Vorgehensweise

1 Klicken Sie auf das Dropdown-Menüsymbol für die Konfiguration und wählen Sie **Verwaltung** aus.

2 Klicken Sie unter „Verwaltung“ auf **Appliance**.

3 Klicken Sie auf **Master neu starten** und dann auf **Neu starten**.

Weiter

Stellen Sie nach dem Neustart von vRealize Log Insight sicher, dass Syslog-Feeds von ESXi nach wie vor in vRealize Log Insight ankommen. Informationen zur Fehlerbehebung finden Sie unter Es gehen keine ESXi-Protokolle mehr in Log Insight ein.

Stellen Sie nach dem Neustart von vRealize Log Insight sicher, dass Syslog-Feeds von ESXi nach wie vor in vRealize Log Insight ankommen. Informationen zur Fehlerbehebung finden Sie im Thema über ESXi-Protokolle im *Log Insight-Administratorhandbuch*.

Ausschalten der virtuellen vRealize Log Insight -Appliance

Um beim Ausschalten eines vRealize Log Insight-Master- oder Worker-Knotens einen Datenverlust zu vermeiden, müssen Sie den Knoten in einer strengen Abfolge von Schritten ausschalten.

Sie müssen die virtuelle vRealize Log Insight-Appliance ausschalten, bevor Sie Änderungen an der virtuellen Hardware der Appliance vornehmen.

Sie können die virtuelle vRealize Log Insight-Appliance über die Menüoption **Betrieb > Gast herunterfahren** in vSphere Client, mithilfe der Konsole der virtuellen Appliance oder durch Herstellung einer SSH-Verbindung zur virtuellen vRealize Log Insight-Appliance und Ausführung eines Befehls ausschalten.

Voraussetzungen

- Wenn Sie eine Verbindung zu einer virtuellen vRealize Log Insight-Appliance unter Verwendung von SSH herstellen möchten, stellen Sie sicher, dass TCP-Port 22 geöffnet ist.
- Stellen Sie sicher, dass Sie über die Root-Benutzer-Anmeldedaten verfügen, um sich bei der virtuellen vRealize Log Insight-Appliance anzumelden.

Vorgehensweise

1. Stellen Sie eine SSH-Verbindung zur vRealize Log Insight-vApp her und melden Sie sich als Root-Benutzer an.
2. Führen Sie zum Ausschalten der virtuellen vRealize Log Insight-Appliance `shutdown –h now` aus.

Weiter

Sie können sicher Änderungen an der virtuellen Hardware der virtuellen vRealize Log Insight-Appliance vornehmen.

Hinzufügen von Arbeitsspeicher und CPU zur virtuellen vRealize Log Insight -Appliance

Sie können die Arbeitsspeichermenge und die Anzahl der CPUs ändern, die einer virtuellen vRealize Log Insight-Appliance nach der Bereitstellung zugeteilt werden.

Sie müssen möglicherweise die Ressourcenzuweisung anpassen, beispielsweise wenn die Anzahl von Ereignissen in Ihrer Umgebung zunimmt.

Voraussetzungen

- Melden Sie sich bei vSphere Client als Benutzer mit Berechtigungen zum Ändern der Hardware der virtuellen Maschinen in Ihrer Umgebung an.
- Fahren Sie die virtuelle vRealize Log Insight-Appliance sicher herunter. Siehe „Ausschalten der virtuellen vRealize Log Insight-Appliance“, auf Seite 43.

Vorgehensweise

1. Klicken Sie mit der rechten Maustaste in der vSphere Client-Bestandsliste auf die virtuelle vRealize Log Insight-Maschine und wählen Sie **Einstellungen bearbeiten** aus.
2. Klicken Sie auf der Registerkarte **Hardware** auf **Hinzufügen**.
3. Passen Sie die CPU- und Arbeitsspeichermenge nach Bedarf an.
4. Überprüfen Sie die Informationen und klicken Sie auf **Beenden**.

5 Klicken Sie auf **OK**, um Ihre Änderungen zu speichern und das Dialogfeld zu schließen.

Wenn Sie die virtuelle vRealize Log Insight-Appliance einschalten, beginnt die virtuelle Maschine mit der Nutzung der neuen Ressourcen.

Einstellen des Versands von Protokollierungsdaten an VMware

Wenn Sie nicht mehr am Programm zur Verbesserung der Kundenzufriedenheit teilnehmen möchten, können Sie die Übertragung anonymisierter Protokollierungsdaten an VMware einstellen.

Sollten Sie Fragen oder Anliegen in Bezug auf das Programm zur Verbesserung der Kundenzufriedenheit für vRealize Log Insight haben, wenden Sie sich bitte an li-info@vmware.com.

Voraussetzungen

Vergewissern Sie sich, dass Sie bei der Web-Benutzeroberfläche von vRealize Log Insightals Benutzer mit der Berechtigung **Admin bearbeiten** angemeldet sind. Das URL-Format lautet https://*log-insight-host*, wobei *log-insight-host* die IP-Adresse oder der Hostname der virtuellen vRealize Log Insight-Appliance ist.

Vorgehensweise

1 Klicken Sie auf das Dropdown-Menüsymbol für die Konfiguration und wählen Sie **Verwaltung** aus.

2 Klicken Sie unter „Konfiguration“ auf **Allgemein**.

3 Deaktivieren Sie im Bereich „Programm zur Verbesserung der Kundenzufriedenheit“ das Kontrollkästchen **Im Rahmen des Programms zur Verbesserung der Benutzerfreundlichkeit wöchentliche Protokollierungsdaten an VMware senden**.

4 Klicken Sie auf **Speichern**.

vRealize Log Insight versendet keine Protokollierungsdaten mehr an VMware.

Konfigurieren von vRealize Log Insight-Clustern 3

Sie können Knoten eines vRealize Log Insight-Clusters hinzufügen, entfernen und aktualisieren.

Hinweis Das WAN-Clustering wird von vRealize Log Insight nicht unterstützt. Aktuelle Versionen von vRealize Log Insight unterstützen das WAN-Clustering nicht (dies wird auch als Geo-Clustering, Hochverfügbarkeits-Clustering oder Remote-Clustering bezeichnet). Alle Knoten im Cluster müssen in demselben Layer 2-LAN bereitgestellt werden. Darüber hinaus müssen die unter Ports und externe Schnittstellen beschriebenen Ports zwischen den Knoten geöffnet sein, um eine ordnungsgemäße Kommunikation zu gewährleisten.

Dieses Kapitel behandelt die folgenden Themen:

- „Hinzufügen eines Worker-Knotens zu einem vRealize Log Insight-Cluster“, auf Seite 45
- „Entfernen eines Worker-Knotens aus einem vRealize Log Insight-Cluster“, auf Seite 49
- „Aktivieren des integrierten Lastausgleichsdiensts“, auf Seite 50

Hinzufügen eines Worker-Knotens zu einem vRealize Log Insight - Cluster

Stellen Sie eine neue Instanz der virtuellen Log Insight-Appliance bereit und fügen Sie sie einem vorhandenen Log Insight-Master-Knoten hinzu.

Vorgehensweise

1 Bereitstellen der virtuellen vRealize Log Insight-Appliance auf Seite 46

Laden Sie die virtuelle vRealize Log Insight-Appliance herunter. VMware verteilt die virtuelle vRealize Log Insight-Appliance als `.ova`-Datei. Stellen Sie die virtuelle vRealize Log Insight-Appliance mithilfe von vSphere Client bereit.

2 Hinzufügen zu einer vorhandenen Bereitstellung auf Seite 48

Nach Bereitstellung und Einrichtung eines eigenständigen vRealize Log Insight-Knotens können Sie eine neue vRealize Log Insight-Instanz bereitstellen und diese dem vorhandenen Knoten hinzufügen, um einen vRealize Log Insight -Cluster zu bilden.

Bereitstellen der virtuellen vRealize Log Insight -Appliance

Laden Sie die virtuelle vRealize Log Insight-Appliance herunter. VMware verteilt die virtuelle vRealize Log Insight-Appliance als `.ova`-Datei. Stellen Sie die virtuelle vRealize Log Insight-Appliance mithilfe von vSphere Client bereit.

Voraussetzungen

- Vergewissern Sie sich, dass Sie über eine Kopie der `.ova`-Datei der virtuellen vRealize Log Insight-Appliance verfügen.
- Vergewissern Sie sich, dass Sie über die Berechtigungen verfügen, die OVF-Vorlagen in der Bestandsliste bereitzustellen.
- Überprüfen Sie, ob Ihre Umgebung über genügend Ressourcen verfügt, um die Mindestanforderungen der virtuellen vRealize Log Insight-Appliance zu erfüllen. Weitere Informationen hierzu finden Sie unter Mindestanforderungen.
- Die Dimensionierungsempfehlungen für die virtuelle Appliance müssen von Ihnen gelesen und verstanden werden. Siehe Dimensionierung der virtuellen Log Insight-Appliance.

Vorgehensweise

1 Wählen Sie in vSphere Client die Option **Datei > OVF-Vorlage bereitstellen**.

2 Folgen Sie den Eingabeaufforderungen im Assistenten zum Bereitstellen von OVF-Vorlagen.

3 Wählen Sie auf der Seite „Bereitstellungskonfiguration“ die Größe der virtuellen vRealize Log Insight-Appliance auf der Basis der Größe der Umgebung, für die Sie Protokolle erfassen möchten.

Klein ist die Mindestanforderung für Produktionsumgebungen.

Während der Bereitstellung der virtuellen Appliance können Sie die Größe der Appliance wie folgt auswählen.

Option	Protokollaufnahmerate	vCPUs	Arbeitsspeicher	IOPS	Syslog-Verbindungen	Ereignisse pro Sekunde
Extra klein	6GB/Tag	2	4 GB	75	20	400
Klein	30GB/Tag	4	8 GB	500	100	2000
Mittel	75GB/Tag	8	16 GB	1000	250	5000
Groß	225 GB/Tag	16	32 GB	1500	750	15,000

Hinweis Sie können einen Syslog-Aggregator verwenden, um die Anzahl der Syslog-Verbindungen zu erhöhen, die Ereignisse an vRealize Log Insight senden. Die Höchstanzahl der Ereignisse pro Sekunde ist jedoch fest und unabhängig vom Einsatz des Syslog-Aggregators. Eine vRealize Log Insight-Instanz lässt sich nicht als Syslog-Aggregator verwenden.

Hinweis Wenn Sie **Groß** wählen, müssen Sie die virtuelle Hardware auf der virtuellen Maschine von vRealize Log Insight nach der Bereitstellung aktualisieren.

4 Wählen Sie auf der Seite „Festplattenformat“ ein Festplattenformat.

- **Thick-Provision Lazy-Zeroed** erstellt eine virtuelle Festplatte im Standard-Thick-Format. Der für die virtuelle Festplatte erforderliche Speicherplatz wird dann zugeteilt, wenn die virtuelle Festplatte erstellt wird. Die Daten, die auf dem physischen Gerät verbleiben, werden nicht während des Anlegens, sondern zu einem späteren Zeitpunkt während der ersten Schreibvorgänge der virtuellen Appliance gelöscht.
- **Thick-Provision Eager-Zeroed** erstellt einen Typ einer virtuellen Festplatte im Thick-Format, der Clusterfunktionen, wie z. B. Fault Tolerance, unterstützt. Der Speicher, den die virtuelle Festplatte benötigt, wird beim Erstellen zugewiesen. Im Gegensatz zum Flat-Format werden die auf dem physischen Gerät verbleibenden Daten durch Nullbyte ersetzt („zeroed out“), wenn die virtuelle Festplatte erstellt wird. Das Anlegen von Festplatten in diesem Format kann wesentlich länger dauern als das Anlegen anderer Festplattentypen.

  Wichtig Stellen Sie, soweit möglich, die virtuelle vRealize Log Insight-Appliance mit Festplatten vom Typ Thick-Provisioned, Eager-Zeroed bereit, um Leistung und Betrieb der virtuellen Appliance zu optimieren.

- **Thin Provision** erstellt eine Festplatte im Thin-Format. Die Festplatte vergrößert sich mit anwachsendem Volumen der auf ihr gespeicherten Daten. Wenn Ihr Speichergerät keine Festplatten vom Typ Thick-Provisioning unterstützt oder Sie ungenutzten Speicherplatz auf der virtuellen vRealize Log Insight-Appliance einsparen möchten, stellen Sie die virtuelle Appliance mit Festplatten vom Typ Thin-Provisioning bereit.

Hinweis Das Verkleinern von Festplatten auf der virtuellen vRealize Log Insight-Appliance wird nicht unterstützt und kann zu Datenbeschädigung oder -verlust führen.

5 (Optional) Stellen Sie auf der Seite „Eigenschaften“ die Netzwerkparameter für die virtuelle vRealize Log Insight-Appliance ein.

Wenn Sie keine Netzwerkeinstellungen wie IP-Adresse, DNS-Server und Gateway vornehmen, verwendet vRealize Log Insight DHCP, um diese Einstellungen vorzunehmen.

Vorsicht Geben Sie nicht mehr als zwei Domänennamenserver an. Wenn Sie mehr als zwei Domänennamenserver angeben, werden alle konfigurierten Domänennamenserver in der virtuellen vRealize Log Insight-Appliance ignoriert.

Trennen Sie Domänennamenserver mit einem Komma.

6 (Optional) Stellen Sie auf der Seite „Eigenschaften“ das Root-Kennwort für die virtuelle vRealize Log Insight-Appliance ein.

7 Folgen Sie den Eingabeaufforderungen, um die Bereitstellung abzuschließen.

Informationen zur Bereitstellung virtueller Appliances finden Sie im *Benutzerhandbuch für die Bereitstellung von vApps und virtuellen Appliances*.

Nach dem Einschalten der virtuellen Appliance beginnt eine Initialisierung. Das Abschließen der Initialisierung kann unter Umständen mehrere Minuten dauern. Am Ende des Vorgangs erfolgt ein Neustart der virtuellen Appliance.

8 Gehen Sie zur Registerkarte **Konsole** und überprüfen Sie die IP-Adresse der virtuellen vRealize Log Insight-Appliance.

IP-Adresspräfix	Beschreibung
https://	Die DHCP-Konfiguration in der virtuellen Appliance ist korrekt.
http://	Die DHCP-Konfiguration in der virtuellen Appliance ist fehlgeschlagen. a Schalten Sie die virtuelle vRealize Log Insight-Appliance aus. b Klicken Sie mit der rechten Maustaste auf die virtuelle Appliance und wählen Sie **Einstellungen bearbeiten**. c Legen Sie eine statische IP-Adresse für die virtuelle Appliance fest.

Weiter

- Konfigurieren Sie das Root-Kennwort in der Konsole der virtuellen Appliance, um SSH-Verbindungen zur virtuellen vRealize Log Insight-Appliance zu aktivieren. Näheres hierzu finden Sie unter Konfigurieren des SSH-Root-Kennworts für die virtuelle Log Insight-Appliance.
- Informationen zum Konfigurieren einer eigenständigen Bereitstellung von vRealize Log Insight finden Sie unter Konfigurieren einer neuen Bereitstellung von Log Insight.

  Die vRealize Log Insight-Web-Benutzeroberfläche ist über https://*log-insight-host*/ verfügbar, wobei *log-insight-host* die IP-Adresse oder der Hostname der virtuellen vRealize Log Insight-Appliance ist.

Hinzufügen zu einer vorhandenen Bereitstellung

Nach Bereitstellung und Einrichtung eines eigenständigen vRealize Log Insight-Knotens können Sie eine neue vRealize Log Insight-Instanz bereitstellen und diese dem vorhandenen Knoten hinzufügen, um einen vRealize Log Insight -Cluster zu bilden.

vRealize Log Insight ermöglicht eine horizontale Skalierung durch den Einsatz mehrerer virtueller Appliance-Instanzen. Dies ermöglicht eine lineare Skalierung des Aufnahmedurchsatzes, erhöht die Abfrageleistung und sorgt für Hochverfügbarkeit bei der Aufnahme. Im Cluster-Modus bietet vRealize Log Insight Master- und Worker-Knoten. Master- und Worker-Knoten sind für eine Teilmenge von Daten verantwortlich. Master-Knoten können alle Teilmengen von Daten abfragen und die Ergebnisse aggregieren.

Wichtig Es wird nachdrücklich empfohlen, dass Sie in einem vRealize Log Insight-Cluster mindestens drei Knoten konfigurieren, um Aufnahme, Konfiguration und eine hohe Verfügbarkeit des Benutzerspeicherplatzes zu bieten.

Voraussetzungen

- Notieren Sie in vSphere Client die IP-Adresse der virtuellen vRealize Log Insight-Worker-Appliance.
- Sie müssen die IP-Adresse oder den Hostnamen der virtuellen vRealize Log Insight-Master-Appliance kennen.
- Stellen Sie sicher, dass Sie über ein Administratorkonto auf der virtuellen vRealize Log Insight-Master-Appliance verfügen.
- Stellen Sie sicher, dass die Versionen der vRealize Log Insight-Master- und Worker-Knoten synchron sind. Fügen Sie einem vRealize Log Insight-Master-Knoten einer neueren Version keinen vRealize Log Insight-Worker-Knoten einer älteren Version hinzu.
- Sie müssen die Uhrzeit der virtuellen vRealize Log Insight-Appliance mit einem NTP-Server synchronisieren. Siehe Synchronisieren der Uhrzeit der virtuellen Log Insight-Appliance.
- Weitere Informationen über unterstützte Browserversionen finden Sie in den Versionshinweise zu vRealize Log Insight.

Vorgehensweise

1 Verwenden Sie einen unterstützten Browser, um zur Web-Benutzeroberfläche des vRealize Log Insight-Workers zu navigieren.

Das URL-Format lautet https://*log_insight-host*/, wobei *log_insight-host* die IP-Adresse oder der Hostname der virtuellen vRealize Log Insight-Worker-Appliance ist.

Der Erstkonfigurationsassistent wird geöffnet.

2 Klicken Sie auf **Hinzufügen zu einer vorhandenen Bereitstellung**.

3 Geben Sie die IP-Adresse oder den Hostnamen des vRealize Log Insight-Masters ein und klicken Sie auf **Los**.

Der Worker sendet eine Anfrage an den vRealize Log Insight-Master, der vorhandenen Bereitstellung beizutreten.

4 Klicken Sie auf den Link **Klicken Sie hier, um auf die Seite „Clusterverwaltung“ zuzugreifen**.

5 Melden Sie sich als Administrator an.

Die Cluster-Seite wird geladen.

6 Klicken Sie auf **Zulassen**.

Der Worker wird der vorhandenen Bereitstellung hinzugefügt und vRealize Log Insight wird als Cluster betrieben.

Weiter

- Stellen Sie, um einen weiteren Worker hinzuzufügen, eine neue vRealize Log Insight-Instanz bereit und fügen Sie diese über den Startassistenten dem Cluster hinzu.
- Wiederholen Sie das Verfahren, um mindestens zwei vRealize Log Insight-Worker-Knoten hinzuzufügen.

Entfernen eines Worker-Knotens aus einem vRealize Log Insight -Cluster

Sie können einen Worker-Knoten, der nicht mehr richtig arbeitet, aus einem vRealize Log Insight-Cluster entfernen und einem anderen Cluster hinzufügen oder eine eigenständige Bereitstellung starten. Entfernen Sie keine Worker-Knoten, die ordnungsgemäß arbeiten, aus einem Cluster.

Das Entfernen eines Knotens führt zu Datenverlust. Wenn ein Knoten entfernt werden muss, stellen Sie sicher, dass er gesichert wurde. Warten Sie 30 Minuten nach dem Hinzufügen neuer Knoten, bevor Sie Knoten entfernen.

Voraussetzungen

- Vergewissern Sie sich, dass Sie bei der Web-Benutzeroberfläche von vRealize Log Insightals Benutzer mit der Berechtigung **Admin bearbeiten** angemeldet sind. Das URL-Format lautet https://*log-insight-host*, wobei *log-insight-host* die IP-Adresse oder der Hostname der virtuellen vRealize Log Insight-Appliance ist.
- Wenn Sie einen externen Lastausgleichsdienst verwenden, nehmen Sie den Knoten aus diesem Modul heraus, bevor Sie ihn in den Wartungsmodus versetzen.

Vorgehensweise

1 Klicken Sie auf das Dropdown-Menüsymbol für die Konfiguration und wählen Sie **Verwaltung** aus.

2 Klicken Sie unter „Verwaltung“ auf **Cluster**.

3 Suchen Sie in der Tabelle „Worker“ den gewünschten Knoten und klicken Sie auf und dann auf **Weiter**.

Der Knoten befindet sich jetzt im Wartungsmodus.

HINWEIS Ein Knoten im Wartungsmodus erhält weiterhin Protokolle.

4 Klicken Sie auf , um den Knoten zu entfernen.

vRealize Log Insight entfernt den Knoten aus dem Cluster und sendet eine E-Mail-Benachrichtigung.

Beispiel:

Weiter

Navigieren Sie zur Web-Benutzeroberfläche des entfernten Knotens, um diesen zu konfigurieren. Sie können den Knoten einem anderen bestehenden vRealize Log Insight-Cluster hinzufügen oder eine neue eigenständige Bereitstellung starten.

Aktivieren des integrierten Lastausgleichsdiensts

Sie können den integrierten Lastausgleichsdienst in einem vRealize Log Insight-Cluster aktivieren, um sicherzustellen, dass der eingehende Aufnahmeverkehr von vRealize Log Insight akzeptiert wird, selbst wenn einige vRealize Log Insight-Knoten nicht verfügbar sein sollten.

Es wird dringend empfohlen, in einer vRealize Log Insight-Clusterumgebung den integrierten Lastausgleichsdienst zu aktivieren.

Der integrierte Lastausgleichsdienst stellt sicher, dass der eingehende Aufnahmeverkehr von vRealize Log Insight akzeptiert wird, selbst wenn einige vRealize Log Insight-Knoten nicht verfügbar sein sollten. Außerdem verteilt der integrierte Lastausgleichsdienst den eingehenden Datenverkehr gleichmäßig auf alle verfügbaren vRealize Log Insight-Knoten. vRealize Log Insight-Clients, die sowohl die Web-Benutzeroberfläche als auch die Aufnahme (über Syslog oder die Ingestion-API) verwenden, sollten sich über die IP-Adresse des integrierten Lastausgleichsdiensts mit vRealize Log Insight verbinden.

Für den integrierten Lastausgleichsdienst müssen alle vRealize Log Insight-Knoten im selben Layer-2-Netzwerk liegen, beispielsweise hinter demselben Switch, oder auf sonstige Weise in der Lage sein, ARP-Anforderungen untereinander zu versenden oder zu empfangen. Die IP-Adresse des integrierten Lastausgleichsdiensts muss so eingerichtet sein, dass jeder vRealize Log Insight-Knoten über sie Datenverkehr empfangen kann. Das bedeutet üblicherweise, dass sich die IP-Adresse des integrierten Lastausgleichsdiensts im selben Subnetz wie die physische Adresse der vRealize Log Insight-Knoten befindet. Nach der Konfiguration der IP-Adresse des integrierten Lastausgleichsdiensts versuchen Sie einen Ping von einem anderen Netzwerk aus, um sicherzugehen, dass sie erreicht werden kann.

Um zukünftige Änderungen und Upgrades möglichst einfach zu gestalten, können Clients auf einen FQDN verweisen, der die IP-Adresse des integrierten Lastausgleichsdiensts auflöst, anstatt direkt auf die IP-Adresse des integrierten Lastausgleichsdiensts zu verweisen.

Voraussetzungen

- Konfigurieren Sie mindestens drei Knoten in einem vRealize Log Insight-Cluster.
- Überprüfen Sie, dass sich alle vRealize Log Insight-Knoten und die angegebene IP-Adresse des integrierten Lastausgleichsdiensts im selben Netzwerk befinden.

- Die Master- und Worker-Knoten von vRealize Log Insight müssen dieselben Zertifikate aufweisen. Andernfalls lehnen die vRealize Log Insight-Agenten, die für die Verbindung mit SSL konfiguriert sind, die Verbindung ab. Setzen Sie beim Hochladen eines von einer Zertifizierungsstelle signierten Zertifikats auf Master- und Worker-Knoten von vRealize Log Insight den allgemeinen Namen während der Zertifikatserstellungsanfrage auf die IP-Adresse des integrierten Lastausgleichsdiensts. Weitere Informationen hierzu finden Sie unter „Generieren einer Zertifizierungsanforderung“, auf Seite 32.
- Sie müssen die Uhrzeit der virtuellen vRealize Log Insight-Appliance mit einem NTP-Server synchronisieren. Siehe Synchronisieren der Uhrzeit der virtuellen Log Insight-Appliance.

Vorgehensweise

1 Klicken Sie auf das Dropdown-Menüsymbol für die Konfiguration und wählen Sie **Verwaltung** aus.

2 Klicken Sie unter „Verwaltung“ auf **Cluster**.

3 Wählen Sie unter „Konfiguration“ die Option **Integrierten Lastausgleichsdienst aktivieren** und geben Sie die virtuelle IP-Adresse für den integrierten Lastausgleich ein.

4 (Optional) Um Benutzern von vRealize Log Insight den Zugriff auf den Cluster über einen FQDN zu ermöglichen, verweisen Sie die Clients auf den FQDN anstatt direkt auf die konfigurierte IP-Adresse des integrierten Lastausgleichsdiensts.

5 Klicken Sie auf **Speichern**.

Konfigurieren von vRealize Log Insight-Agenten

4

Sie können den Status von vRealize Log Insight-Agenten überwachen und Agentengruppen erstellen, um zu ermöglichen, dass Konfigurationsänderungen auf mehrere Agenten angewendet werden.

Dieses Kapitel behandelt die folgenden Themen:

- „Überwachen des Status von vRealize Log Insight Windows- und Linux-Agenten“, auf Seite 53
- „Arbeiten mit Agentengruppen“, auf Seite 54

Überwachen des Status von vRealize Log Insight Windows- und Linux-Agenten

Sie können den Status der Windows- und Linux-Agenten von vRealize Log Insight überwachen und aktuelle Statistiken über deren Betrieb anzeigen.

Nur Agenten, die für das Senden von Daten über CFAPI konfiguriert sind, werden auf der Seite „Agenten“ angezeigt. Agenten, die gemäß ihrer Konfiguration Daten über syslog senden, werden wie andere Syslog-Quellen auf der Seite „Hosts“ angezeigt.

Voraussetzungen

Vergewissern Sie sich, dass Sie bei der Web-Benutzeroberfläche von vRealize Log Insightals Benutzer mit der Berechtigung **Admin bearbeiten** angemeldet sind. Das URL-Format lautet https://*log-insight-host*, wobei *log-insight-host* die IP-Adresse oder der Hostname der virtuellen vRealize Log Insight-Appliance ist.

Vorgehensweise

1 Klicken Sie auf das Dropdown-Menüsymbol für die Konfiguration und wählen Sie **Verwaltung** aus.

2 Klicken Sie unter „Verwaltung“ auf **Agenten**.

Weiter

Anhand der Informationen auf der Seite „Agenten“ können Sie den Betrieb der installierten Windows- und Linux-Agenten von vRealize Log Insight überwachen.

Arbeiten mit Agentengruppen

Mithilfe von vRealize Log Insight-Server können Sie Agenten über die Benutzeroberfläche der Anwendung konfigurieren. Agenten fragen den vRealize Log Insight-Server regelmäßig ab, um zu ermitteln, ob neue Konfigurationen verfügbar sind.

Sie können Agenten, für die dieselbe Konfiguration erforderlich ist, in Gruppen zusammenfassen. Zum Beispiel können Sie alle vRealize Log Insight-Windows-Agenten getrennt von den vRealize Log Insight-Linux-Agenten in Gruppen zusammenfassen.

Im Menü **Alle Agenten** werden vorhandene Agentengruppen von Inhaltspaketen automatisch aufgeführt. Die aufgeführten Agenten sind mit von Ihnen schon installierten Inhaltspaketen verknüpft (zum Beispiel das vSphere-Inhaltspaket), die Agentengruppen verwenden.

Inhaltspaketgruppen sind schreibgeschützt.

Nur Konfigurationsabschnitte, die mit `[winlog]`, `[filelog]` und `[parser]` beginnen, werden in Inhaltspaketen verwendet. Zusätzliche Abschnitte werden nicht als Bestandteil eines Inhaltspakets exportiert. Nur einzeilige Kommentare (Zeilen, die mit `;` beginnen) in den Abschnitten `[winlog]`, `[filelog]` und `[parser]` bleiben in einem Inhaltspaket erhalten.

Im Agenten-Administratorhandbuch zu vRealize Log Insight finden Sie Informationen zum Konfigurieren von Agenten, einschließlich Informationen zum Zusammenführen von Konfigurationen zwischen lokalen und serverseitigen Konfigurationen.

- Zusammenführen von Agentengruppen-Konfigurationen auf Seite 54

  Mit Agentengruppen können Agenten Teil von mehreren Gruppen sein und der Standardgruppe *Alle Agenten* angehören, was eine zentrale Konfiguration ermöglicht.

- Erstellen einer Agentengruppe auf Seite 55

  Sie können eine Gruppe von Agenten erstellen, die mit denselben Parametern konfiguriert werden.

- Bearbeiten einer Agentengruppe auf Seite 55

  Sie können den Namen und die Beschreibung einer Agentengruppe bearbeiten, die Filter ändern und die Konfiguration bearbeiten.

- Hinzufügen einer Inhaltspaket-Agentengruppe als Agentengruppe auf Seite 56

  Sie können Ihren aktiven Gruppen eine Agentengruppe hinzufügen, die als Teil eines Inhaltspakets definiert wurde, und auf die Gruppe eine Agentenkonfiguration anwenden.

- Löschen einer AgentengruppeLöschen einer Agentengruppe auf Seite 56

  Sie können eine Agentengruppe löschen, um sie aus der Liste der aktiven Gruppen zu entfernen.

Zusammenführen von Agentengruppen-Konfigurationen

Mit Agentengruppen können Agenten Teil von mehreren Gruppen sein und der Standardgruppe *Alle Agenten* angehören, was eine zentrale Konfiguration ermöglicht.

Das Zusammenführen erfolgt serverseitig, die sich ergebende Konfiguration wird mit der agentenseitigen Konfiguration zusammengeführt. Die zusammengeführte Konfiguration ergibt sich aus den folgenden Regeln.

- Die einzelnen Gruppenkonfigurationen haben eine höhere Priorität und Vorrang vor den Gruppeneinstellungen „Alle Agenten“.
- Die Gruppenkonfiguration „Alle Agenten“ hat Vorrang vor der lokalen Konfiguration.

- Mit Ausnahme der Gruppe „Alle Agenten“ können Sie keine Abschnitte mit demselben Namen in verschiedenen Gruppen konfigurieren. Die Abschnitte in den einzelnen Gruppen haben jedoch eine höhere Priorität.

Die zusammengeführte Konfiguration wird in der agentenseitigen Datei `liagent-effective.ini` gespeichert.

Erstellen einer Agentengruppe

Sie können eine Gruppe von Agenten erstellen, die mit denselben Parametern konfiguriert werden.

Voraussetzungen

Vergewissern Sie sich, dass Sie bei der Web-Benutzeroberfläche von vRealize Log Insightals Benutzer mit der Berechtigung **Admin bearbeiten** angemeldet sind. Das URL-Format lautet https://*log-insight-host*, wobei *log-insight-host* die IP-Adresse oder der Hostname der virtuellen vRealize Log Insight-Appliance ist.

Vorgehensweise

1. Klicken Sie auf das Dropdown-Menüsymbol für die Konfiguration und wählen Sie **Verwaltung** aus.
2. Klicken Sie unter „Verwaltung“ auf **Agenten**.
3. Klicken Sie im Menü **Alle Agenten** auf **Neue Gruppe**.
4. Geben Sie einen eindeutigen Namen und eine Beschreibung für die Agentengruppe an und klicken Sie auf **Neue Gruppe**.

   Die Agentengruppe wird erstellt und in der Liste **Alle Agenten** eingeblendet, sie wird aber nicht gespeichert.
5. Legen Sie einen oder mehrere der folgenden Filter für die Agentengruppe fest.
   - IP-Adresse
   - Hostname
   - Version
   - Betriebssystem

   Sie können zum Beispiel den Betriebssystemfilter `contains` auswählen und den Wert `windows` zum Kennzeichnen aller Ihrer Windows-Agenten für die Konfiguration festlegen.

   Bevor Sie einen Filter festlegen, sind alle Agenten aufgeführt.
6. Legen Sie die Agentenkonfigurationswerte im Bereich „Agentenkonfiguration“ fest und klicken Sie auf **Neue Gruppe speichern**.

Die Agentenkonfiguration wird nach dem nächsten Abfrageintervall angewendet.

Bearbeiten einer Agentengruppe

Sie können den Namen und die Beschreibung einer Agentengruppe bearbeiten, die Filter ändern und die Konfiguration bearbeiten.

Voraussetzungen

Vergewissern Sie sich, dass Sie bei der Web-Benutzeroberfläche von vRealize Log Insightals Benutzer mit der Berechtigung **Admin bearbeiten** angemeldet sind. Das URL-Format lautet https://*log-insight-host*, wobei *log-insight-host* die IP-Adresse oder der Hostname der virtuellen vRealize Log Insight-Appliance ist.

Vorgehensweise

1 Klicken Sie auf das Dropdown-Menüsymbol für die Konfiguration und wählen Sie **Verwaltung** aus.

2 Klicken Sie unter „Verwaltung“ auf **Agenten**.

3 Wählen Sie im Menü **Alle Agenten** den Namen der entsprechenden Agentengruppe aus und klicken Sie auf das Bleistiftsymbol, um sie zu bearbeiten.

4 Nehmen Sie die gewünschten Änderungen vor.

Zu bearbeitende Option	Aktion
Name oder **Beschreibung**	Nehmen Sie die erforderlichen Änderungen vor und klicken Sie auf **Speichern**.
Filter oder **Konfiguration**	Nehmen Sie die erforderlichen Änderungen vor und klicken Sie auf **Gruppe speichern**.

Hinzufügen einer Inhaltspaket-Agentengruppe als Agentengruppe

Sie können Ihren aktiven Gruppen eine Agentengruppe hinzufügen, die als Teil eines Inhaltspakets definiert wurde, und auf die Gruppe eine Agentenkonfiguration anwenden.

Voraussetzungen

Vergewissern Sie sich, dass Sie bei der Web-Benutzeroberfläche von vRealize Log Insightals Benutzer mit der Berechtigung **Admin bearbeiten** angemeldet sind. Das URL-Format lautet https://*log-insight-host*, wobei *log-insight-host* die IP-Adresse oder der Hostname der virtuellen vRealize Log Insight-Appliance ist.

Vorgehensweise

1 Klicken Sie auf das Dropdown-Menüsymbol für die Konfiguration und wählen Sie **Verwaltung** aus.

2 Klicken Sie unter „Verwaltung“ auf **Agenten**.

3 Wählen Sie im Menü **Alle Agenten** eine Agentenvorlage für die Liste „Verfügbare Vorlagen“ aus.

4 Klicken Sie auf **Vorlage kopieren** zum Kopieren der Inhaltspaket-Agentengruppe in Ihre aktiven Gruppen.

5 Klicken Sie auf **Kopieren**.

6 Wählen Sie die erforderlichen Filter aus und klicken Sie auf **Neue Gruppe speichern**.

Die Inhaltspaket-Agentengruppe wird den aktiven Gruppen hinzugefügt und die Agenten werden entsprechend den von Ihnen angegebenen Filtern konfiguriert.

Löschen einer AgentengruppeLöschen einer Agentengruppe

Sie können eine Agentengruppe löschen, um sie aus der Liste der aktiven Gruppen zu entfernen.

Voraussetzungen

Vergewissern Sie sich, dass Sie bei der Web-Benutzeroberfläche von vRealize Log Insightals Benutzer mit der Berechtigung **Admin bearbeiten** angemeldet sind. Das URL-Format lautet https://*log-insight-host*, wobei *log-insight-host* die IP-Adresse oder der Hostname der virtuellen vRealize Log Insight-Appliance ist.

Vorgehensweise

1 Klicken Sie auf das Dropdown-Menüsymbol für die Konfiguration und wählen Sie **Verwaltung** aus.

2 Klicken Sie unter „Verwaltung“ auf **Agenten**.

3 Wählen Sie im Menü **Alle Agenten** den Namen der zu löschenden Agentengruppe durch Klicken auf das Symbol X neben ihrem Namen aus.

4 Klicken Sie auf **Löschen**.

Die Agentengruppe wird aus der Liste der aktiven Gruppen entfernt.

Verwalten von vRealize Log Insight-Benutzerkonten

5

Administratoren können Benutzerkonten und Rollen erstellen, um Zugriff auf die Web-Benutzeroberfläche von vRealize Log Insight zu ermöglichen.

Nur Benutzer mit der Berechtigung Admin bearbeiten können Benutzerkonten erstellen und bearbeiten. Benutzer können allerdings ohne die Berechtigung Admin bearbeiten ihr eigenes E-Mail- und Kontokennwort ändern.

Dieses Kapitel behandelt die folgenden Themen:

- „Benutzerverwaltung – Übersicht“, auf Seite 59
- „Rollenbasierte Zugriffssteuerung“, auf Seite 60
- „Erstellen eines neuen Benutzerkontos in vRealize Log Insight“, auf Seite 60
- „Hinzufügen eines Active Directory-Benutzers zu vRealize Log Insight“, auf Seite 61
- „Hinzufügen einer Active Directory-Gruppe zu vRealize Log Insight“, auf Seite 62
- „Definieren eines Datensatzes“, auf Seite 64
- „Erstellen und Ändern von Rollen“, auf Seite 65
- „Löschen eines Benutzerkontos aus vRealize Log Insight“, auf Seite 65
- „Aktivieren der Benutzerauthentifizierung über Active Directory“, auf Seite 66

Benutzerverwaltung – Übersicht

Systemadministratoren nutzen eine Kombination aus Benutzeranmeldungen, einer rollenbasierten Zugriffssteuerung, Berechtigungen und Datensätzen zur Verwaltung von vRealize Log Insight-Benutzern. Mit der rollenbasierten Zugriffssteuerung können Administratoren Benutzer und die Aufgaben, die diese wahrnehmen, verwalten.

Bei den Rollen handelt es sich um Berechtigungssätze, die zur Durchführung bestimmter Aufgaben erforderlich sind. Systemadministratoren definieren Rollen als Teil der Definition von Sicherheitsrichtlinien und weisen die Rollen dann den Benutzern zu. Zum Ändern der Berechtigungen und der Aufgaben, die einer bestimmten Aufgabe zugewiesen sind, aktualisiert der Systemadministrator die Rolleneinstellungen. Die aktualisierten Einstellungen treten für alle Benutzer, die der Rolle zugewiesen sind, in Kraft.

- Um einem Benutzer die Durchführung einer Aufgabe zu gestatten, weist der Systemadministrator dem Benutzer die Rolle zu.
- Um einen Benutzer von der Durchführung einer Aufgabe abzuhalten, hebt der Systemadministrator die Zuweisung der Rolle zum Benutzer wieder auf.

Die Verwaltung des Zugriffs, der Rollen und Berechtigungen für jeden Benutzer basiert auf dem jeweiligen Benutzeranmeldungskonto. Jedem Benutzer können verschiedene Rollen und Berechtigungen zugewiesen werden.

Benutzern, die bestimmte Objekte nicht sehen bzw. nicht darauf zugreifen können, oder die bestimmte Operationen nicht durchführen können, wurden die entsprechenden Berechtigungen dafür nicht zugewiesen.

Rollenbasierte Zugriffssteuerung

Mit der rollenbasierten Zugriffssteuerung können Systemadministratoren den Benutzerzugriff auf vRealize Log Insight sowie Aufgaben steuern, die Benutzer nach erfolgreicher Anmeldung durchführen können. Um die rollenbasierte Zugriffssteuerung zu implementieren, ordnen Systemadministratoren Berechtigungen und Rollen mit oder aus Benutzeranmeldekonten zu oder heben diese auf.

Benutzer Systemadministratoren können den Zugriff und die Aktionen aller Benutzer steuern, indem sie für das Anmeldekonto des Benutzers Berechtigungen und Rollen gewähren oder diese aufheben.

Berechtigungen Mit Berechtigungen werden die zulässigen Aktionen in vRealize Log Insight gesteuert. Berechtigungen werden auf bestimmte Verwaltungs- oder Benutzeraufgaben in vRealize Log Insight angewendet. Beispiel: Sie können die Berechtigung **Admin anzeigen** gewähren, um einem Benutzer zu erlauben, auf die administrativen vRealize Log Insight-Einstellungen zuzugreifen.

Datensätze Datensätze bestehen aus einer Gruppe von Filtern. Sie können Datensätze verwenden, um Benutzern Zugriff auf bestimmten Inhalt zu ermöglichen, indem ein Datensatz mit einer Rolle verknüpft wird.

Rollen Rollen sind Sammlungen aus Berechtigungen und Datensätzen, die mit Benutzern verbunden werden können. Mit Rollen können alle für eine auszuführende Aufgabe erforderlichen Berechtigungen auf bequeme Weise gebündelt werden. Ein Benutzer kann mehreren Rollen zugewiesen werden.

Erstellen eines neuen Benutzerkontos in vRealize Log Insight

Benutzer, denen die Rolle „Super Admin“ zugewiesen wird, können Benutzerkonten anlegen, um so den Zugang zur vRealize Log Insight-Web-Benutzeroberfläche zu gewähren.

Voraussetzungen

Vergewissern Sie sich, dass Sie bei der Web-Benutzeroberfläche von vRealize Log Insightals Benutzer mit der Berechtigung **Admin bearbeiten** angemeldet sind. Das URL-Format lautet https://*log-insight-host*, wobei *log-insight-host* die IP-Adresse oder der Hostname der virtuellen vRealize Log Insight-Appliance ist.

Vorgehensweise

1 Klicken Sie auf das Dropdown-Menüsymbol für die Konfiguration und wählen Sie **Verwaltung** aus.

2 Klicken Sie unter „Verwaltung“ auf **Zugriffsteuerung**.

3 Klicken Sie auf **Benutzer und Gruppen**.

4 Klicken Sie auf **Neuer Benutzer**.

5 Wählen Sie im Dropdown-Menü **Authentifizierung** die Option **Standard (integriert)** aus.

6 Geben Sie einen Benutzernamen und eine E-Mail-Adresse ein.

Die E-Mail-Adresse ist optional.

7 Wählen Sie rechts in der Liste **Rollen** eine oder mehrere vordefinierte benutzerdefinierte Benutzerrollen aus.

Option	Beschreibung
Benutzer	Benutzer können auf alle Funktionen von vRealize Log Insight zugreifen, um Protokollereignisse anzuzeigen, Abfragen zum Suchen und Filtern von Protokollen auszuführen, Inhaltspakete in ihren eigenen Benutzerbereich zu importieren, Warnungsabfragen hinzufügen und ihre eigenen Benutzerkonten verwalten, um ihr Kennwort oder ihre E-Mail-Adresse zu ändern. Benutzer haben keinen Zugriff auf die Verwaltungsoptionen, können keine Inhalte für andere Benutzer freigeben, können die Konten von anderen Benutzern nicht ändern und können ein Inhaltspaket nicht als Inhaltspaket installieren.
Dashboard-Benutzer	Dashboard-Benutzer können nur die Seite „Dashboards“ von vRealize Log Insight verwenden.
Leseberechtigung-Admin	Leseberechtigung-Admin-Benutzer können Admin-Informationen anzeigen, haben vollständigen Benutzerzugriff und können freigegebenen Inhalt bearbeiten.
Super-Admin	Super-Admin-Benutzer können auf alle Funktionen von vRealize Log Insight zugreifen, können vRealize Log Insightverwalten und die Konten aller Benutzer verwalten.

8 Kopieren Sie das Kennwort aus dem Textfeld **Kennwort** und stellen Sie es dem Benutzer zur Verfügung.

9 Klicken Sie auf **Speichern**.

Hinzufügen eines Active Directory-Benutzers zu vRealize Log Insight

Sie können Active Directory-Benutzern (AD) erlauben, sich mit ihren Domänen-Anmeldedaten bei vRealize Log Insight anzumelden.

Wenn Sie die AD-Unterstützung in vRealize Log Insight aktivieren, konfigurieren Sie einen Domänennamen und geben Sie einen Bindungsbenutzer an, der zur Domäne gehört. vRealize Log Insight verwendet den Bindungsbenutzer, um die Verbindung zur AD-Domäne und das Vorhandensein von AD-Benutzern und -Gruppen zu überprüfen.

AD-Benutzer, die Sie vRealize Log Insight hinzufügen, müssen entweder der Domäne des Bindungsbenutzers oder einer Domäne, die der Domäne des Bindungsbenutzers vertraut, angehören.

Voraussetzungen

- Vergewissern Sie sich, dass Sie bei der Web-Benutzeroberfläche von vRealize Log Insight als Benutzer mit der Berechtigung **Admin bearbeiten** angemeldet sind. Das URL-Format lautet `https://log-insight-host`, wobei `log-insight-host` die IP-Adresse oder der Hostname der virtuellen vRealize Log Insight-Appliance ist.
- Vergewissern Sie sich, dass die AD-Unterstützung konfiguriert ist. Siehe „Aktivieren der Benutzerauthentifizierung über Active Directory“, auf Seite 66.

Vorgehensweise

1 Klicken Sie auf das Dropdown-Menüsymbol für die Konfiguration und wählen Sie **Verwaltung** aus.

2 Klicken Sie unter „Verwaltung“ auf **Zugriffsteuerung**.

3 Klicken Sie auf **Neuer Benutzer**.

4 Wählen Sie im Dropdown-Menü **Authentifizierungsmethode** die Option **Active Directory**.

Der von Ihnen bei der Konfiguration der AD-Unterstützung angegebene Standarddomänenname wird im Textfeld **Domäne** angezeigt. Wenn Sie Benutzer der Standarddomäne hinzufügen, dürfen Sie den Domänennamen nicht ändern.

5 (Optional) Wenn Sie einen Benutzer aus einer Domäne, die der Standarddomäne vertraut, hinzufügen möchten, geben Sie den Namen der vertrauenden Domäne im Textfeld **Domäne** ein.

6 Geben Sie den Namen eines Domänenbenutzers ein.

7 Wählen Sie rechts in der Liste **Rollen** eine oder mehrere vordefinierte benutzerdefinierte Benutzerrollen aus.

Option	Beschreibung
Benutzer	Benutzer können auf alle Funktionen von vRealize Log Insight zugreifen, um Protokollereignisse anzuzeigen, Abfragen zum Suchen und Filtern von Protokollen auszuführen, Inhaltspakete in ihren eigenen Benutzerbereich zu importieren, Warnungsabfragen hinzufügen und ihre eigenen Benutzerkonten verwalten, um ihr Kennwort oder ihre E-Mail-Adresse zu ändern. Benutzer haben keinen Zugriff auf die Verwaltungsoptionen, können keine Inhalte für andere Benutzer freigeben, können die Konten von anderen Benutzern nicht ändern und können ein Inhaltspaket nicht als Inhaltspaket installieren.
Dashboard-Benutzer	Dashboard-Benutzer können nur die Seite „Dashboards“ von vRealize Log Insight verwenden.
Leseberechtigung-Admin	Leseberechtigung-Admin-Benutzer können Admin-Informationen anzeigen, haben vollständigen Benutzerzugriff und können freigegebenen Inhalt bearbeiten.
Super-Admin	Super-Admin-Benutzer können auf alle Funktionen von vRealize Log Insight zugreifen, können vRealize Log Insightverwalten und die Konten aller Benutzer verwalten.

8 Klicken Sie auf **Speichern**.

vRealize Log Insight prüft, ob der Benutzer in der von Ihnen angegebenen Domäne oder deren vertrauenswürdigen Domänen vorhanden ist. Wenn der Benutzer nicht vorhanden ist, werden Sie durch ein Dialogfeld darauf hingewiesen, dass vRealize Log Insight den Benutzer nicht bestätigen kann. Sie können den Benutzer ohne Bestätigung speichern oder den Vorgang abbrechen und den Benutzernamen korrigieren.

Von Ihnen hinzugefügte AD-Benutzer können sich mit ihren Domänen-Anmeldedaten bei vRealize Log Insight anmelden.

Hinzufügen einer Active Directory-Gruppe zu vRealize Log Insight

Anstatt einzelne Domänenbenutzer hinzuzufügen, können Sie Domänengruppen hinzufügen, um den Benutzern die Anmeldung bei vRealize Log Insight zu gestatten.

Wenn Sie die AD-Unterstützung in vRealize Log Insight aktivieren, konfigurieren Sie einen Domänennamen und geben Sie einen Bindungsbenutzer an, der zur Domäne gehört. vRealize Log Insight verwendet den Bindungsbenutzer, um die Verbindung zur AD-Domäne und das Vorhandensein von AD-Benutzern und -Gruppen zu überprüfen.

Die AD-Gruppen, die Sie vRealize Log Insight hinzufügen, müssen entweder der Domäne des Bindungsbenutzers oder einer Domäne, der die Domäne des Bindungsbenutzers vertraut, angehören.

Voraussetzungen

- Vergewissern Sie sich, dass Sie bei der Web-Benutzeroberfläche von vRealize Log Insight als Benutzer mit der Berechtigung **Admin bearbeiten** angemeldet sind. Das URL-Format lautet `https://log-insight-host`, wobei `log-insight-host` die IP-Adresse oder der Hostname der virtuellen vRealize Log Insight-Appliance ist.
- Vergewissern Sie sich, dass die AD-Unterstützung konfiguriert ist. Siehe „Aktivieren der Benutzerauthentifizierung über Active Directory“, auf Seite 66.

Vorgehensweise

1 Klicken Sie auf das Dropdown-Menüsymbol für die Konfiguration und wählen Sie **Verwaltung** aus.

2 Klicken Sie unter „Verwaltung“ auf **Zugriffsteuerung**.

3 Klicken Sie auf **Benutzer und Gruppen**.

4 Klicken Sie unter „Active Directory-Gruppen“ auf **Neue Gruppe**.

Der von Ihnen bei der Konfiguration der AD-Unterstützung angegebene Standarddomänenname wird im Textfeld **Domäne** angezeigt. Wenn Sie Gruppen zur Standarddomäne hinzufügen, dürfen Sie den Domänennamen nicht ändern.

5 (Optional) Wenn Sie eine Gruppe aus einer Domäne, die der Standarddomäne vertraut, hinzufügen möchten, geben Sie den Namen der vertrauenden Domäne in das Textfeld **Domäne** ein.

6 Geben Sie den Namen der AD-Gruppe ein, die Sie hinzufügen möchten.

7 Wählen Sie rechts in der Liste **Rollen** eine oder mehrere vordefinierte benutzerdefinierte Benutzerrollen aus.

Option	Beschreibung
Benutzer	Benutzer können auf alle Funktionen von vRealize Log Insight zugreifen, um Protokollereignisse anzuzeigen, Abfragen zum Suchen und Filtern von Protokollen auszuführen, Inhaltspakete in ihren eigenen Benutzerbereich zu importieren, Warnungsabfragen hinzufügen und ihre eigenen Benutzerkonten verwalten, um ihr Kennwort oder ihre E-Mail-Adresse zu ändern. Benutzer haben keinen Zugriff auf die Verwaltungsoptionen, können keine Inhalte für andere Benutzer freigeben, können die Konten von anderen Benutzern nicht ändern und können ein Inhaltspaket nicht als Inhaltspaket installieren.
Dashboard-Benutzer	Dashboard-Benutzer können nur die Seite „Dashboards“ von vRealize Log Insight verwenden.
Leseberechtigung-Admin	Leseberechtigung-Admin-Benutzer können Admin-Informationen anzeigen, haben vollständigen Benutzerzugriff und können freigegebenen Inhalt bearbeiten.
Super-Admin	Super-Admin-Benutzer können auf alle Funktionen von vRealize Log Insight zugreifen, können vRealize Log Insightverwalten und die Konten aller Benutzer verwalten.

8 Klicken Sie auf **Speichern**.

vRealize Log Insight verifiziert, ob die AD-Gruppe in der Domäne, die Sie angegeben haben, oder in einer vertrauenswürdigen Domäne vorhanden ist. Wenn die Gruppe nicht gefunden wird, wird Ihnen ein Dialogfeld eingeblendet, in dem Sie darüber informiert werden, dass vRealize Log Insight diese Gruppe nicht verifizieren kann. Sie können die Gruppe ohne Verifizierung speichern oder den Vorgang abbrechen und den Gruppennamen korrigieren.

Benutzer, die zu der AD-Gruppe gehören, die Sie hinzugefügt haben, können sich über ihr Domänenkonto bei vRealize Log Insight anmelden. Sie verfügen dann über dieselbe Berechtigungsstufe wie die Gruppe, der sie angehören.

Definieren eines Datensatzes

Sie können einen Datensatz definieren, um Benutzerzugriff auf bestimmte Inhalte zu gewährleisten.

Voraussetzungen

Vergewissern Sie sich, dass Sie bei der Web-Benutzeroberfläche von vRealize Log Insightals Benutzer mit der Berechtigung **Admin bearbeiten** angemeldet sind. Das URL-Format lautet https://*log-insight-host*, wobei *log-insight-host* die IP-Adresse oder der Hostname der virtuellen vRealize Log Insight-Appliance ist.

Vorgehensweise

1 Klicken Sie auf das Dropdown-Menüsymbol für die Konfiguration und wählen Sie **Verwaltung** aus.

2 Klicken Sie unter „Verwaltung“ auf **Zugriffsteuerung**.

3 Klicken Sie auf **Datensätze**.

4 Klicken Sie auf **Neuer Datensatz**.

5 Klicken Sie auf **Filter hinzufügen**.

6 Verwenden Sie das erste Dropdown-Menü, um ein beliebiges innerhalb von vRealize Log Insight definiertes Feld zu verwenden.

   Beispiel: **hostname**.

   Die Liste enthält alle definierten Felder, die statisch verfügbar sind, Inhaltspaketen und in benutzerdefiniertem Inhalt.

   Hinweis Numerische Felder enthalten zusätzliche Operatoren, die in Zeichenfolgenfeldern nicht vorkommen: =, >, <, >= und <=. Diese Operatoren führen numerische Vergleiche aus. Durch ihre Verwendung können andere Ergebnisse als bei der Verwendung von Zeichenfolgenoperatoren erzielt werden. Beispiel: Der Filter **response_time = `02`** ergibt als Treffer ein Ereignis, das ein Feld **response_time** mit einem Wert von 2 enthält. Der Filter **response_time enthält `02`** ergibt nicht denselben Treffer.

7 Verwenden Sie das zweite Dropdown-Menü, um den Vorgang auszuwählen, der auf das im ersten Dropdown-Menü ausgewählte Feld angewendet werden soll.

   Wählen Sie zum Beispiel **enthält**. Der Filter **enthält** gleicht vollständige Token ab: Wenn Sie z. B. den Suchbegriff „err“ eingeben, werden keine Übereinstimmungen mit `error` ausgegeben.

8 Geben Sie im Textfeld rechts neben dem Dropdown-Menü für den Filter den Wert ein, den Sie als Filter verwenden möchten.

   Sie können mehrere Werte verwenden. Der Operator zwischen diesen Werten ist ODER.

   Hinweis Das Textfeld ist nicht verfügbar, wenn Sie im zweiten Dropdown-Menü den Operator **ist vorhanden** auswählen.

9 (Optional) Klicken Sie auf **Filter hinzufügen**, um weitere Filter hinzuzufügen.

10 Klicken Sie auf **Speichern**.

Weiter

Ordnen Sie einer Benutzerrolle einen Datensatz zu. Weitere Informationen hierzu finden Sie unter „Erstellen und Ändern von Rollen“, auf Seite 65.

Erstellen und Ändern von Rollen

Sie können benutzerdefinierte Rollen erstellen oder vordefinierte Rollen ändern, um den Benutzern die Durchführung bestimmter Aufgaben sowie den Zugriff auf bestimmte Inhalte zu gestatten.

Voraussetzungen

Vergewissern Sie sich, dass Sie bei der Web-Benutzeroberfläche von vRealize Log Insightals Benutzer mit der Berechtigung **Admin bearbeiten** angemeldet sind. Das URL-Format lautet https://*log-insight-host*, wobei *log-insight-host* die IP-Adresse oder der Hostname der virtuellen vRealize Log Insight-Appliance ist.

Vorgehensweise

1 Klicken Sie auf das Dropdown-Menüsymbol für die Konfiguration und wählen Sie **Verwaltung** aus.

2 Klicken Sie unter „Verwaltung“ auf **Zugriffsteuerung**.

3 Klicken Sie auf **Rollen**.

4 Klicken Sie auf **Neue Rolle** oder auf , um eine vorhandene Rolle zu bearbeiten.

Sie müssen zunächst die Rollen „Super Admin“ und „Benutzer“ klonen, bevor Sie sie bearbeiten können.

5 Ändern Sie die Textfelder **Name** und **Beschreibung**.

6 Wählen Sie eine oder mehrere Berechtigung(en) aus der Liste „Berechtigungen“ aus.

Option	Beschreibung
Admin bearbeiten	Damit können Admin-Informationen und -Einstellungen bearbeitet werden
Admin anzeigen	Damit können Admin-Informationen und -Einstellungen angezeigt werden
Freigegebene bearbeiten	Damit können freigegebene Inhalte bearbeitet werden
Analytics	Damit kann die Interaktive Analyse verwendet werden
Dashboard	Damit können Dashboards angezeigt werden

7 (Optional) Wählen Sie rechts aus der Liste **Datensätze** einen Datensatz aus, welcher der Benutzerrolle zugewiesen werden soll.

8 Klicken Sie auf **Speichern**.

Löschen eines Benutzerkontos aus vRealize Log Insight

Benutzerkonten können über die Benutzeroberfläche für Administratoren von vRealize Log Insight gelöscht werden.

Voraussetzungen

Vergewissern Sie sich, dass Sie bei der Web-Benutzeroberfläche von vRealize Log Insightals Benutzer mit der Berechtigung **Admin bearbeiten** angemeldet sind. Das URL-Format lautet https://*log-insight-host*, wobei *log-insight-host* die IP-Adresse oder der Hostname der virtuellen vRealize Log Insight-Appliance ist.

Vorgehensweise

1 Klicken Sie auf das Dropdown-Menüsymbol für die Konfiguration und wählen Sie **Verwaltung** aus.

2 Klicken Sie unter „Verwaltung“ auf **Zugriffsteuerung**.

3 Klicken Sie auf **Benutzer und Gruppen**.

4 Aktivieren Sie das Kontrollkästchen neben dem Benutzernamen, der gelöscht werden soll.

5 Klicken Sie auf das Symbol **Löschen** .

Aktivieren der Benutzerauthentifizierung über Active Directory

vRealize Log Insight verfügt über eine integrierte Authentifizierungsmethode, die Sie zur Benutzerauthentifizierung verwenden können.

Wenn Sie mithilfe der integrierten Authentifizierungsmethode neue Benutzerkonten erstellen, stellen Sie den Benutzern Kennwörter zur Verfügung, die sie für die Anmeldung bei vRealize Log Insight verwenden müssen.

Damit die Benutzer sich nicht mehrere Kennwörter merken müssen, können Sie die Unterstützung der Active Directory-Authentifizierung aktivieren.

Voraussetzungen

Vergewissern Sie sich, dass Sie bei der Web-Benutzeroberfläche von vRealize Log Insightals Benutzer mit der Berechtigung **Admin bearbeiten** angemeldet sind. Das URL-Format lautet https://*log-insight-host*, wobei *log-insight-host* die IP-Adresse oder der Hostname der virtuellen vRealize Log Insight-Appliance ist.

Vorgehensweise

1 Klicken Sie auf das Dropdown-Menüsymbol für die Konfiguration und wählen Sie **Verwaltung** aus.

2 Klicken Sie unter „Konfiguration“ auf **Authentifizierung**.

3 Aktivieren Sie das Kontrollkästchen **Active Directory-Unterstützung aktivieren**.

4 Geben Sie im Textfeld **Standarddomäne** einen Domänennamen ein.

Beispiel: `firmenname.com`.

Hinweis Im Standarddomänen-Textfeld darf nicht mehr als eine Domäne eingegeben werden. Wird der Standarddomäne, die Sie angegeben haben, von anderen Domänen vertraut, verwendet vRealize Log Insight die Standarddomäne und den Bindungsbenutzer, um AD-Benutzer und -Gruppen in den vertrauenden Domänen zu überprüfen.

Außerdem können Sie nicht zu einer anderen Domäne auf einer Instanz wechseln, die schon Benutzer und Gruppen enthält.

---

5 Geben Sie die Anmeldedaten eines der Standarddomäne angehörenden Bindungsbenutzers ein.

vRealize Log Insight verwendet die Standarddomäne und den Bindungsbenutzer, um AD-Benutzer und -Gruppen in der Standarddomäne und in Domänen, die der Standarddomäne vertrauen, zu überprüfen.

6 Klicken Sie auf **Speichern**.

Weiter

Erteilen Sie AD-Benutzern und -Gruppen Berechtigungen, um auf die aktuelle Instanz von vRealize Log Insight zuzugreifen. Weitere Informationen hierzu finden Sie unter „Hinzufügen eines Active Directory-Benutzers zu vRealize Log Insight“, auf Seite 61.

Konfigurieren des für Active Directory zu verwendenden Protokolls

Sie können das Protokoll konfigurieren, das beim Verbinden mit Active Directory verwendet werden soll. Wenn sich vRealize Log Insight mit einem Active Directory verbindet, wird standardmäßig zunächst ein Nicht-SSL-LDAP-Verbindungsaufbau, und dann erforderlichenfalls ein SSL-LDAP-Verbindungsaufbau versucht.

Wenn Sie die Active Directory-Kommunikation auf ein bestimmtes Protokoll beschränken oder die Reihenfolge der für die Verbindungsversuche zu verwendenden Protokolle ändern möchten, müssen Sie zusätzliche Konfigurationen in der virtuellen vRealize Log Insight-Appliance vornehmen.

Voraussetzungen

- Stellen Sie sicher, dass Sie über die Root-Benutzer-Anmeldedaten verfügen, um sich bei der virtuellen vRealize Log Insight-Appliance anzumelden. Siehe „Konfigurieren des SSH-Root-Kennworts für die virtuelle Log Insight-Appliance“, auf Seite 16.
- Um SSH-Verbindungen zu aktivieren, überprüfen Sie zunächst, ob der TCP-Port 22 geöffnet ist.

Vorgehensweise

1. Stellen Sie eine SSH-Verbindung zur virtuellen vRealize Log Insight-Appliance her und melden Sie sich als Root-Benutzer an.
2. Navigieren Sie zum folgenden Speicherort: `/storage/var/loginsight/config`
3. Suchen Sie die neueste Konfigurationsdatei mit der höchsten [Ziffer]:`/storage/core/loginsight/config/loginsight-config.xml#[number]`
4. Kopieren Sie die neueste Konfigurationsdatei: `/storage/core/loginsight/config/loginsight-config.xml#[number]`
5. Erhöhen Sie die [Ziffer] und speichern Sie die Datei am folgenden Speicherort: `/storage/core/loginsight/config/loginsight-config.xml#[number + 1]`
6. Öffnen Sie die Datei zum Bearbeiten.
7. Fügen Sie im Abschnitt `Authentication` die Zeile hinzu, die der Konfiguration entspricht, die Sie anwenden möchten:

Option	Beschreibung
`<ad-protocols value="LDAP" />`	Speziell, um LDAP ohne SSL zu verwenden
`<ad-protocols value="LDAPS" />`	Speziell für die ausschließliche Verwendung von LDAP mit SSL
`<ad-protocols value="LDAP,LDAPS" />`	Speziell, um erst LDAP und dann LDAP mit SSL zu verwenden
`<ad-protocols value="LDAPS,LDAP" />`	Speziell, um erst LDAPS und dann LDAP ohne SSL zu verwenden

   Wenn Sie kein Protokoll auswählen, versucht vRealize Log Insight zunächst LDAP und dann LDAP mit SSL zu verwenden.
8. Speichern und schließen Sie die Datei.
9. Führen Sie den Befehl `service loginsight restart` aus.

Überwachen von vRealize Log Insight 6

Sie können die virtuelle Appliance von vRealize Log Insight und die Hosts und Geräte überwachen, die Protokollereignisse zu vRealize Log Insight senden.

Dieses Kapitel behandelt die folgenden Themen:

- „Prüfen des Systemzustands der virtuellen vRealize Log Insight-Appliance“, auf Seite 69
- „Überwachen von Protokollereignisse sendenden Hosts“, auf Seite 70

Prüfen des Systemzustands der virtuellen vRealize Log Insight - Appliance

Sie können die verfügbaren Ressourcen und aktiven Abfragen auf der virtuellen vRealize Log Insight-Appliance überprüfen und aktuelle Statistiken über den Betrieb von vRealize Log Insight aufrufen.

Voraussetzungen

Vergewissern Sie sich, dass Sie bei der Web-Benutzeroberfläche von vRealize Log Insightals Benutzer mit der Berechtigung **Admin bearbeiten** angemeldet sind. Das URL-Format lautet https://*log-insight-host*, wobei *log-insight-host* die IP-Adresse oder der Hostname der virtuellen vRealize Log Insight-Appliance ist.

Vorgehensweise

1 Klicken Sie auf das Dropdown-Menüsymbol für die Konfiguration und wählen Sie **Verwaltung** aus.

2 Klicken Sie unter „Verwaltung“ auf **System-Monitor**.

3 Wenn vRealize Log Insight als Cluster ausgeführt wird, klicken Sie auf **Ressourcen anzeigen für** und wählen Sie den Knoten aus, den Sie überwachen möchten.

4 Klicken Sie auf die Schaltflächen auf der Seite „Systemüberwachung“, um die benötigten Informationen anzuzeigen.

Option	Beschreibung
Ressourcen	Anzeigen von Informationen über CPU, Arbeitsspeicher, IOPS (Lese- und Schreibvorgänge) und Speichernutzung auf der virtuellen vRealize Log Insight-Appliance. Die Diagramme auf der rechten Seite zeigen historische Daten der letzten 24 Stunden und werden alle fünf Minuten aktualisiert. Die Diagramme auf der linken Anzeige enthalten Informationen der letzten fünf Minuten und werden alle drei Sekunden aktualisiert.
Aktive Abfragen	Anzeigen von Informationen zu den derzeit in vRealize Log Insight aktiven Abfragen.
Statistiken	Anzeigen von Statistiken zu den Protokollaufnahmevorgängen und -raten. Um detaillierte Statistiken anzuzeigen, klicken Sie auf **Erweiterte Statistik anzeigen**.

Weiter

Sie können mit den Informationen der Seite „Systemüberwachung“ Ressourcen auf der virtuellen vRealize Log Insight-Appliance verwalten.

Überwachen von Protokollereignisse sendenden Hosts

Sie können eine Liste mit allen Hosts und Geräten anzeigen, die Protokollereignisse an vRealize Log Insight senden, um diese zu überwachen.

Voraussetzungen

Vergewissern Sie sich, dass Sie bei der Web-Benutzeroberfläche von vRealize Log Insightals Benutzer mit der Berechtigung **Admin bearbeiten** angemeldet sind. Das URL-Format lautet https://*log-insight-host*, wobei *log-insight-host* die IP-Adresse oder der Hostname der virtuellen vRealize Log Insight-Appliance ist.

Vorgehensweise

1 Klicken Sie auf das Dropdown-Menüsymbol für die Konfiguration und wählen Sie **Verwaltung** aus.

2 Klicken Sie unter „Verwaltung“ auf **Hosts**.

HINWEIS Wenn Sie einen vCenter Server zum Senden von Ereignissen und Warnungen konfiguriert haben, die einzelnen ESXi-Hosts jedoch nicht zum Senden von Protokollen konfiguriert haben, werden in der Liste „Hostname“ nicht nur die vCenter Server-Hosts, sondern auch die einzelnen ESXi-Hosts als Quelle aufgelistet.

Einbinden von vRealize Log Insight in VMware-Produkte 7

vRealize Log Insight kann in andere VMware-Produkte eingebunden werden, um Ereignisse und Protokolldaten zu verwenden und eine bessere Einsicht in Ereignisse zu bieten, die in einer virtuellen Umgebung auftreten.

Integration in VMware vSphere

vRealize Log Insight-Administratorbenutzer können vRealize Log Insight so einrichten, dass alle zwei Minuten eine Verbindung mit vCenter Server hergestellt wird und Ereignis-, Warnungs-und Aufgabendaten dieser vCenter Server-Systeme gesammelt werden. Außerdem kann vRealize Log Insight ESXi-Hosts über vCenter Server konfigurieren. Weitere Informationen hierzu finden Sie unter „Verbinden von vRealize Log Insight mit einer vSphere-Umgebung“, auf Seite 72.

Integration in VMware vRealize Operations Manager

Sie können vRealize Log Insight in vRealize Operations Manager vApp und vRealize Operations Manager Installable integrieren. Die Integration in die Installable-Version erfordert zusätzliche Änderungen an der Konfiguration von vRealize Operations Manager. Informationen zur Konfiguration von vRealize Operations Manager Installable zur Integration in vRealize Log Insightfinden Sie in der Anleitung *Erste Schritte für Log Insight*.

vRealize Log Insight und vRealize Operations Manager lassen sich auf zwei unabhängige Weisen integrieren.

Benachrichtigungsereignisse

vRealize Log Insight-Administratorbenutzer können vRealize Log Insight so einrichten, dass auf von Ihnen erstellten Abfragen basierende Benachrichtigungsereignisse an vRealize Operations Manager gesendet werden. Diese Benachrichtigungsereignisse sind in vRealize Operations Manager keine Warnungen und haben keinen Einfluss auf die Werte der Badges „Systemzustand“, „Risiko“ oder „Effizienz“. Weitere Informationen hierzu finden Sie unter „Konfigurieren von vRealize Log Insight zum Senden von Benachrichtigungsereignissen an vRealize Operations Manager“, auf Seite 79.

Kontextbezogener Start

Kontextbezogener Start ist eine Funktion in vRealize Operations Manager, die es Ihnen ermöglicht, in einem bestimmten Kontext eine externe Anwendung per URL zu starten. Der Kontext wird durch das aktive Benutzeroberflächenelement und die Objektauswahl definiert. Über den kontextbezogenen Start kann der vRealize Log Insight-Adapter einer Reihe verschiedener Ansichten innerhalb der benutzerdefinierten Benutzeroberfläche und der

vSphere-Benutzeroberfläche von vRealize Operations Manager Menüelemente hinzufügen. Weitere Informationen hierzu finden Sie unter „Aktivieren des kontextbezogenen Starts für vRealize Log Insight in vRealize Operations Manager“, auf Seite 84.

HINWEIS Benachrichtigungsereignisse hängen nicht von der Konfiguration des kontextbezogenen Starts ab. Sie können Benachrichtigungsereignisse auch dann von vRealize Log Insight an vRealize Operations Manager senden, wenn Sie die Funktion Kontextbezogener Start nicht aktivieren.

Wenn sich die Umgebung verändert, können Administratorbenutzer von vRealize Log Insight vSphere-Systeme ändern, hinzufügen oder aus vRealize Log Insight entfernen, die vRealize Operations Manager-Instanz ändern oder entfernen, an die Warnungsbenachrichtigungen gesendet werden, und die zur Verbindung von vSphere-Systemen und vRealize Operations Manager verwendeten Kennwörter ändern.

Dieses Kapitel behandelt die folgenden Themen:

- „Verbinden von vRealize Log Insight mit einer vSphere-Umgebung“, auf Seite 72
- „Konfigurieren von vRealize Log Insight zum Senden von Benachrichtigungsereignissen an vRealize Operations Manager“, auf Seite 79
- „Aktivieren der Active Directory-Integration von vRealize Log Insight und vRealize Operations Manager“, auf Seite 81
- „Hinzufügen einer Suchdomäne“, auf Seite 81
- „Installieren des vRealize Log Insight-Adapters in der Standalone-Version von vRealize Operations Manager“, auf Seite 82
- „vRealize Operations Manager-Inhaltspaket für vRealize Log Insight“, auf Seite 83
- „Aktivieren des kontextbezogenen Starts für vRealize Log Insight in vRealize Operations Manager“, auf Seite 84
- „Deaktivieren des kontextbezogenen Starts für vRealize Log Insight in vRealize Operations Manager“, auf Seite 87
- „Entfernen des vRealize Log Insight-Adapters aus einer vRealize Operations Manager-Instanz“, auf Seite 88

Verbinden von vRealize Log Insight mit einer vSphere-Umgebung

Bevor Sie vRealize Log Insight für die Erfassung von Warnungs-, Ereignis- und Aufgabendaten aus Ihrer vSphere-Umgebung konfigurieren, müssen Sie vRealize Log Insight mit einem oder mehreren vCenter Server-Systemen verbinden.

vRealize Log Insight kann zwei Arten von Daten aus vCenter Server-Instanzen und den ESXi-Hosts, die sie verwalten, erfassen.

- Ereignisse, Aufgaben und Warnungen sind strukturierte Daten mit spezifischer Bedeutung. Nach erfolgter Konfiguration ruft vRealize Log Insight Ereignisse, Aufgaben und Warnungen der registrierten vCenter Server-Instanzen ab.
- Protokolle enthalten unstrukturierte Daten, die in vRealize Log Insight analysiert werden können. ESXi-Hosts oder vCenter Server Appliance-Instanzen können ihre Protokolle über Syslog an vRealize Log Insight übermitteln.

Voraussetzungen

- Vergewissern Sie sich, dass Sie für den gewünschten Integrationsgrad über Anmeldedaten mit ausreichenden Rechten verfügen, um die erforderliche Konfiguration am vCenter Server-System und dessen ESXi-Hosts vorzunehmen.

Integrationsgrad	Erforderliche Berechtigungen
Erfassung von Ereignissen, Aufgaben und Alarmen	■ **System.Anzeigen** **Hinweis** **System.Anzeigen** ist eine systemdefinierte Berechtigung. Wenn Sie eine benutzerdefinierte Rolle hinzufügen, ohne ihr Berechtigungen zuzuweisen, wird sie als schreibgeschützte Rolle mit drei systemdefinierten Berechtigungen erstellt: **System.Anonym**, **System.Anzeigen** und **System.Lesen**.
Syslog-Konfiguration auf ESXi-Hosts	■ **Host.Konfiguration.Einstellungen ändern** ■ **Host.Konfiguration.Netzwerkkonfiguration**

Hinweis Sie müssen die Berechtigung für die Ordner der obersten Ebene in der vCenter Server-Bestandsliste konfigurieren und sicherstellen, dass das Kontrollkästchen **An untergeordnete Objekte weitergeben** markiert ist.

- Sie müssen die IP-Adresse oder den Domänennamen des vCenter Server-Systems kennen.
- Vergewissern Sie sich, dass Sie bei der Web-Benutzeroberfläche von vRealize Log Insightals Benutzer mit der Berechtigung **Admin bearbeiten** angemeldet sind. Das URL-Format lautet https://*log-insight-host*, wobei *log-insight-host* die IP-Adresse oder der Hostname der virtuellen vRealize Log Insight-Appliance ist.

Vorgehensweise

1 Klicken Sie auf das Dropdown-Menüsymbol für die Konfiguration und wählen Sie **Verwaltung** aus.

2 Klicken Sie unter „Integration“ auf **vSphere**.

3 Geben Sie die IP-Adresse und die Anmeldedaten für einen vCenter Server ein und klicken Sie auf **Verbindung testen**.

Die Verwendung von Anmeldedaten für das Dienstkonto wird empfohlen.

4 (Optional) Klicken Sie, um einen weiteren vCenter Server zu registrieren, auf **vCenter Server hinzufügen** und wiederholen Sie die Schritte 3 bis 5.

Hinweis Registrieren Sie keine vCenter Server-Systeme mit doppelt vorhandenen Namen oder IP-Adressen. vRealize Log Insight prüft nicht, ob vCenter Server-Namen doppelt vorhanden sind. Sie müssen sicherstellen, dass die Liste der registrierten vCenter Server-Systeme keine doppelten Einträge enthält.

5 Klicken Sie auf **Speichern**.

Weiter

- Starten Sie die Erfassung von Ereignis-, Aufgaben- und Warnungsdaten aus der vCenter Server-Instanz, die Sie registriert haben. Weitere Informationen hierzu finden Sie unter „Konfigurieren von vRealize Log Insight für das Abrufen von Ereignissen, Aufgaben und Warnungen aus vCenter Server-Instanzen“, auf Seite 74.
- Starten Sie die Erfassung von Syslog-Feeds von den durch vCenter Server verwalteten ESXi-Hosts. Weitere Informationen hierzu finden Sie unter „Konfigurieren eines ESXi-Hosts für die Weiterleitung von Protokollereignissen an vRealize Log Insight“, auf Seite 75.

Konfigurieren von vRealize Log Insight für das Abrufen von Ereignissen, Aufgaben und Warnungen aus vCenter Server -Instanzen

Ereignisse, Aufgaben und Warnungen sind strukturierte Daten mit spezifischer Bedeutung. Sie können vRealize Log Insight für die Erfassung von Warnungs-, Ereignis- und Aufgabendaten aus einem oder mehreren vCenter Server-Systemen konfigurieren.

Über die Administrations-Benutzeroberfläche können Sie vRealize Log Insight für die Verbindung mit vCenter Server-Systemen konfigurieren. Die Informationen werden von den vCenter Server-Systemen mithilfe der vSphere Web Services-API abgerufen und in der Web-Benutzeroberfläche von vRealize Log Insight als vSphere-Inhaltspaket angezeigt.

Hinweis vRealize Log Insight kann Warnungs-, Ereignis- und Aufgabendaten nur von vCenter Server 5.1 und höher abrufen.

Voraussetzungen

Vergewissern Sie sich, dass Sie über Anmeldedaten mit **System.View**-Berechtigungen verfügen.

Hinweis Sie müssen die Berechtigung für die Ordner der obersten Ebene in der vCenter Server-Bestandsliste konfigurieren und sicherstellen, dass das Kontrollkästchen **An untergeordnete Objekte weitergeben** markiert ist.

Vorgehensweise

1. Klicken Sie auf das Dropdown-Menüsymbol für die Konfiguration und wählen Sie **Verwaltung** aus.
2. Klicken Sie unter „Integration“ auf **vSphere**.
3. Suchen Sie die vCenter Server-Instanz, aus der Sie Daten erfassen möchten, und aktivieren Sie das Kontrollkästchen **vCenter Server-Ereignisse, -Aufgaben und -Warnungen sammeln**.
4. Klicken Sie auf **Speichern**.

vRealize Log Insight verbindet sich alle zwei Minuten mit vCenter Server und bezieht alle neuen Informationen seit dem letzten Abruf.

Weiter

- Analysieren Sie vSphere-Ereignisse mit dem vSphere-Inhaltspaket oder mittels benutzerdefinierter Abfragen.
- Aktivieren Sie Inhaltspaketwarnungen oder benutzerdefinierte Benachrichtigungen für vSphere.

vRealize Log Insight als Syslog-Server

vRealize Log Insight umfasst einen integrierten Syslog-Server, der während der Ausführung des vRealize Log Insight-Diensts andauernd aktiv ist.

Der Syslog-Server überwacht die Ports 514/TCP, 1514/TCP und 514/UDP und kann Protokollnachrichten anderer Hosts aufnehmen. Vom Syslog-Server aufgenommene Nachrichten können in der vRealize Log Insight-Web-Benutzeroberfläche nahezu in Echtzeit durchsucht werden. Damit vRealize Log Insight die Syslog-Nachrichten akzeptieren kann, dürfen sie nicht größer als 10 KB sein.

Konfigurieren eines ESXi -Hosts für die Weiterleitung von Protokollereignissen an vRealize Log Insight

ESXi-Hosts und vCenter Server Appliance-Instanzen generieren unstrukturierte Protokolldaten, die in vRealize Log Insight analysiert werden können.

Sie verwenden die Verwaltungsschnittstelle von vRealize Log Insight zum Konfigurieren von ESXi-Hosts auf einem registrierten vCenter Server, um Syslog-Daten zu vRealize Log Insight zu senden.

Vorsicht Das Ausführen paralleler Konfigurationsaufgaben kann möglicherweise zu fehlerhaften Syslog-Einstellungen auf dem ESXi-Zielhost führen. Stellen Sie sicher, dass kein anderer Administrator die ESXi-Hosts konfiguriert, die Sie konfigurieren möchten.

Ein vRealize Log Insight-Cluster kann einen Lastausgleichsdienst verwenden, um Syslog-Feeds von ESXi und vCenter Server Appliance auf die einzelnen Knoten des Clusters zu verteilen.

Weitere Informationen über das Filtern von Syslog-Nachrichten auf ESXi-Hosts vor dem Senden von Nachrichten an vRealize Log Insight finden Sie unter *Konfigurieren der Protokollfilterung auf ESXi-Hosts* im Abschnitt Einrichten von ESXi im **Installations- und Einrichtungshandbuch für vSphere**.

Informationen zur Konfiguration von Syslog-Feeds über eine vCenter Server Appliance finden Sie unter „Konfigurieren einer vCenter Server Appliance für das Weiterleiten von Protokollereignissen an vRealize Log Insight“, auf Seite 78.

Hinweis vRealize Log Insight kann Syslog-Daten von ESXi-Hosts der Version 5.0 und höher empfangen.

Bei den Versionen 5.0 und 5.1 von vSphere Web Client wird die Protokollierung nach einem Neustart von vRealize Log Insight unterbrochen oder die Verbindung wird unterbrochen. Führen Sie in solchen Fällen den Konfigurationsvorgang noch einmal aus, um den Protokollierungsvorgang neu zu starten.

Voraussetzungen

- Stellen Sie sicher, dass der vCenter Server, der den ESXi-Host verwaltet, bei Ihrer vRealize Log Insight-Instanz registriert ist.
- Vergewissern Sie sich, dass Ihre Anmeldeinformationen über die erforderlichen Rechte zur Konfiguration von Syslog auf ESXi-Hosts verfügen.
  - **Host.Konfiguration.Erweiterte Einstellungen**
  - **Host.Konfiguration.Sicherheitsprofil und Firewall**

  Hinweis Sie müssen die Berechtigung für die Ordner der obersten Ebene in der vCenter Server-Bestandsliste konfigurieren und sicherstellen, dass das Kontrollkästchen **An untergeordnete Objekte weitergeben** markiert ist.

Vorgehensweise

1. Klicken Sie auf das Dropdown-Menüsymbol für die Konfiguration und wählen Sie **Verwaltung** aus.
2. Klicken Sie unter „Integration“ auf **vSphere**.
3. Suchen Sie die vCenter Server-Instanz, die den ESXi-Host, von dem Sie Syslog-Feeds erhalten möchten, verwaltet.
4. Aktivieren Sie das Kontrollkästchen **ESXi-Hosts für das Versenden von Protokollen an Log Insight konfigurieren**.

   vRealize Log Insight konfiguriert standardmäßig alle erreichbaren ESXi-Hosts der Version 5.0 und höher so, dass sie ihre Protokolle über UDP senden.

5 (Optional) Geben Sie den Hostnamen oder die IP-Adresse eines Lastausgleichsdienstes an, den Sie zum Verteilen von Syslog-Feeds verwenden möchten.

6 (Optional) Um diejenigen ESXi-Hosts, die ihre Protokolle an vRealize Log Insight weiterleiten, oder das zu verwendende Protokoll auszuwählen, klicken Sie auf **Erweiterte Optionen**.

7 Klicken Sie auf **Speichern**.

Manuelle Syslog-Konfiguration über vSphere Web Client

Sie können über vSphere Web Client Syslog auf einem ESXi-Host so konfigurieren, dass Protokollmeldungen an vRealize Log Insight weitergeleitet werden.

Um Protokollmeldungen von mehreren ESXi-Hosts auf dem vCenter Server an vRealize Log Insight weiterzuleiten, müssen Sie jeden einzelnen ESXi-Host konfigurieren.

Hinweis Die Vorgehensweise variiert möglicherweise je nach zu konfigurierendem ESXi-Host und verwendetem vSphere Web Client .

Voraussetzungen

Hinweis Diese Vorgehensweise ist nicht anwendbar, wenn Sie bereits einen ESXi-Host für die Weiterleitung von Protokollereignissen an vRealize Log Insight mithilfe der unter „Konfigurieren eines ESXi-Hosts für die Weiterleitung von Protokollereignissen an vRealize Log Insight“, auf Seite 75 beschriebenen Schritte konfiguriert haben.

- Vergewissern Sie sich, dass Ihre Anmeldeinformationen über die erforderlichen Rechte zur Konfiguration von Syslog auf ESXi-Hosts verfügen.
  - **Host.Konfiguration.Erweiterte Einstellungen**
  - **Host.Konfiguration.Sicherheitsprofil und Firewall**

  Hinweis Sie müssen die Berechtigung für die Ordner der obersten Ebene in der vCenter Server-Bestandsliste konfigurieren und sicherstellen, dass das Kontrollkästchen **An untergeordnete Objekte weitergeben** markiert ist.
- Überprüfen Sie, ob Sie bei dem vCenter Server angemeldet sind, der den ESXi-Host verwaltet, den Sie konfigurieren möchten.

Vorgehensweise

1 Wählen Sie im Objektnavigator den ESXi-Host, den Sie konfigurieren möchten, und klicken Sie auf die Registerkarte **Verwalten**.

2 Klicken Sie auf der Registerkarte **Einstellungen** auf **Erweiterte Systemeinstellungen**.

3 Suchen Sie die Eigenschaft Syslog.global.logHost und klicken Sie auf das Symbol **Bearbeiten** .

4 Ändern Sie die Eigenschaft Syslog.global.logHost so, dass sie auf die IP-Adresse oder den Hostnamen von vRealize Log Insightverweist, und klicken Sie auf **OK**.

   Das URL-Format lautet `tcp|udp|ssl://log_insight-host:514|1514`, wobei *log_insight-host* die IP-Adresse bzw. der Hostname der virtuellen vRealize Log Insight-Appliance ist.

   Hinweis Verwenden Sie Port 514 für UDP- und TCP-Kommunikation und Port 1514 für das SSL-Protokoll.

5 Stellen Sie sicher, dass die Firewall nicht die Kommunikationsports blockiert.

a Klicken Sie auf der Registerkarte **Einstellungen** auf **Sicherheitsprofil** und überprüfen Sie, ob Syslog in der Liste „Ausgehende Verbindungen“ erscheint.

b Wenn Sie Syslog nicht in der Liste „Ausgehende Verbindungen“ sehen, klicken Sie oben rechts auf **Bearbeiten**.

c Scrollen Sie in der Dienste-Liste nach unten, bis Sie den Syslog-Dienst finden, und aktivieren Sie das Kontrollkästchen **Syslog**.

d Klicken Sie auf **OK**.

Manuelle Syslog-Konfiguration per Befehlszeile

Sie können Syslog mit dem Dienstprogramm `esxcli` zum Weiterleiten von Protokollereignissen an vRealize Log Insight konfigurieren.

Sie können den `esxcli`-Befehl in der Konsole eines ESXi-Hosts, in der vSphere-Befehlszeilenschnittstelle oder im vSphere Management Assistant ausführen.

Voraussetzungen

Hinweis Diese Vorgehensweise ist nicht anwendbar, wenn Sie bereits einen ESXi-Host für die Weiterleitung von Protokollereignissen an vRealize Log Insight mithilfe der unter „Konfigurieren eines ESXi-Hosts für die Weiterleitung von Protokollereignissen an vRealize Log Insight“, auf Seite 75 beschriebenen Schritte konfiguriert haben.

- Wenn Sie einen ESXi-Host der Version 5.x konfigurieren möchten, lesen und beachten Sie die Informationen im VMware-Knowledgebase-Artikel Konfiguration von Syslog auf ESXi 5.x (KB 2003322).
- Wenn Sie einen ESXi-Host der Version 4.x konfigurieren möchten, lesen und beachten Sie die Informationen im VMware-Knowledgebase-Artikel Aktivieren von Syslog auf ESXi 3.5 und 4.x (KB 1016621).
- Vergewissern Sie sich, dass Ihre Anmeldeinformationen über die erforderlichen Rechte zur Konfiguration von Syslog auf ESXi-Hosts verfügen.
  - **Host.Konfiguration.Erweiterte Einstellungen**
  - **Host.Konfiguration.Sicherheitsprofil und Firewall**

  Hinweis Sie müssen die Berechtigung für die Ordner der obersten Ebene in der vCenter Server-Bestandsliste konfigurieren und sicherstellen, dass das Kontrollkästchen **An untergeordnete Objekte weitergeben** markiert ist.

Vorgehensweise

1 Öffnen Sie eine ESXi-Shell-Konsolensitzung, in der der Befehl `esxcli` zur Verfügung steht.

Sie können beispielsweise vMA verwenden oder die Sitzung direkt auf dem ESXi-Host öffnen.

2 Führen Sie den folgenden Befehl aus, um die aktuellen Konfigurationsoptionen auf dem Host anzuzeigen:

```
esxcli system syslog config get
```

3 Um eine Host-Konfiguration zu ändern, führen Sie den folgenden Befehl zur Angabe der zu ändernden Optionen aus:

```
esxcli system syslog config set --loghost=tcp|udp|ssl://log_insight-host:514
```

Hinweis Sie müssen `udp` oder `tcp` verwenden. Sie dürfen jedoch nicht beide verwenden.

Der folgende Befehl konfiguriert Remote-Syslog beispielsweise zur Verwendung von `udp` auf Port 514.

```
esxcli system syslog config set --loghost=udp://10.11.12.13:514
```

Um Ihren ESXi-Host für das Weiterleiten von Protokollen an mehrere Endpunkte zu konfigurieren, können Sie die Endpunkte durch Kommata getrennt im Befehl auflisten.

```
esxcli system syslog config set --loghost=udp://10.11.12.13:514,tcp://192.168.100.101:514
```

4 Führen Sie, um sicherzustellen, dass die ESXi-Firewall so konfiguriert ist, dass der Syslog-Datenverkehr den Host verlassen darf, folgende Befehle aus:

```
esxcli network firewall ruleset set --ruleset-id=syslog --enabled=true
esxcli network firewall refresh
```

5 Laden Sie die neue Konfiguration, indem Sie den Befehl `esxcli system syslog reload` ausführen.

Hinweis Wenn Sie diesen Befehl nicht ausführen, wird die Konfigurationsänderung nicht wirksam.

Konfigurieren einer vCenter Server Appliance für das Weiterleiten von Protokollereignissen an vRealize Log Insight

Sie können eine vCenter Server Appliance so konfigurieren, dass diese ihre Protokollmeldungen über Syslog an vRealize Log Insight sendet.

Informationen zur Konfiguration von ESXi-Hosts zur Weiterleitung ihrer Protokolle an vRealize Log Insight finden Sie unter Log Insight mit vCenter Server-Systemen verbinden.

Informationen zur Konfiguration von ESXi-Hosts zur Weiterleitung ihrer Protokolle an vRealize Log Insight finden Sie im Abschnitt *vRealize Log Insight mit vCenter Server 5.1.x-Systemen verbinden* des vRealize Log Insight-Administratorhandbuchs.

Voraussetzungen

- Stellen Sie sicher, dass Sie über die Root-Benutzer-Anmeldedaten für die vCenter Server Appliance verfügen.
- Wenn Sie eine Verbindung zu einer virtuellen vRealize Log Insight-Appliance unter Verwendung von SSH herstellen möchten, stellen Sie sicher, dass TCP-Port 22 geöffnet ist.

Vorgehensweise

1 Stellen Sie eine SSH-Verbindung zum vCenter Server Appliance-Host her und melden Sie sich als Root-Benutzer an.

2 Navigieren Sie zu `/etc/syslog-ng/`.

3 Öffnen Sie die Datei `syslog-ng.conf` zur Bearbeitung und fügen Sie am Ende der Datei den folgenden Text hinzu:

```
source vpxd {
file("/var/log/vmware/vpx/vpxd.log" follow_freq(1) flags(no-parse));
file("/var/log/vmware/vpx/vpxd-alert.log" follow_freq(1) flags(no-parse));
file("/var/log/vmware/vpx/vws.log" follow_freq(1) flags(no-parse));
file("/var/log/vmware/vpx/vmware-vpxd.log" follow_freq(1) flags(no-parse));
```

```
file("/var/log/vmware/vpx/inventoryservice/ds.log" follow_freq(1) flags(no-parse));
};
destination loginsight { udp("<loginsight-host>"); };
log { source(vpxd); destination(loginsight); };
```

Hinweis Sie können `tcp` statt `udp` verwenden.

4 Führen Sie `service syslog restart` aus, um die neue Konfiguration zu laden.

Konfigurieren von vRealize Log Insight zum Senden von Benachrichtigungsereignissen an vRealize Operations Manager

Sie können vRealize Log Insight konfigurieren, um Warnungsbenachrichtigungen an vRealize Operations Manager zu senden.

Sie können vRealize Log Insight in vRealize Operations Manager vApp und vRealize Operations Manager Installable integrieren. Die Integration in die Installable-Version erfordert zusätzliche Änderungen an der Konfiguration von vRealize Operations Manager. Informationen zur Konfiguration von vRealize Operations Manager Installable zur Integration in vRealize Log Insightfinden Sie in der Anleitung *Erste Schritte für Log Insight*.

Bei der Integration von vRealize Log Insight-Warnungen mit vRealize Operations Manager können Sie alle Informationen über Ihre Umgebung in einer einzelnen Benutzeroberfläche anzeigen.

Sie können Benachrichtigungsereignisse von mehreren vRealize Log Insight-Instanzen aus an eine einzelne vRealize Operations Manager-Instanz senden. Sie können den kontextbezogenen Start für eine einzelne vRealize Log Insight-Instanz pro vRealize Operations Manager-Instanz aktivieren.

vRealize Log Insight verwendet die VMware vRealize Operations Manager Suite 6.0 REST-API zum Erstellen von Ressourcen und Beziehungen in vRealize Operations Manager zum Konfigurieren des Adapters für den kontextbezogenen Start. Sie können den älteren HTTP-POST-Adapter zum Erstellen des Adapters für den kontextbezogenen Start verwenden. Dazu müssen Sie derzeit aber POST anstelle von REST als Methode festlegen. In der Datei `loginsight-config-base.xml` finden Sie weitere Informationen dazu.

Voraussetzungen

- Vergewissern Sie sich, dass die Version von vRealize Operations Manager Warnungsbenachrichtigungen von vRealize Log Insight unterstützt. Weitere Informationen zu unterstützten Produktversionen finden Sie unter Produktkompatibilität.

  Hinweis vRealize Log Insight überprüft nicht die Version auf dem Ziel-vRealize Operations Manager und Sie können die Konfiguration der Benachrichtigungen fortsetzen. Die Benachrichtigungsereignisse werden jedoch möglicherweise nicht wie erwartet auf der vRealize Operations Manager-Benutzeroberfläche angezeigt.

- Vergewissern Sie sich je nach Art Ihrer Lizenz von vRealize Operations Manager, dass Sie über die minimal erforderlichen Anmeldedaten verfügen.

vRealize Operations Manager-Lizenz	Minimal erforderliche Anmeldedaten
Standard	Standard-Admin-Anmeldedaten
Advanced oder Enterprise	Anmeldedaten für Anwender mit Leseberechtigung

  Hinweis vRealize Log Insight bietet keine Unterstützung für die Active Directory-Integration mit vRealize Operations Manager.

- Sie müssen die IP-Adresse oder den Hostnamen der Zielinstanz von vRealize Operations Manager kennen.

- Vergewissern Sie sich, dass Sie bei der Web-Benutzeroberfläche von vRealize Log Insightals Benutzer mit der Berechtigung **Admin bearbeiten** angemeldet sind. Das URL-Format lautet https://*log-insight-host*, wobei *log-insight-host* die IP-Adresse oder der Hostname der virtuellen vRealize Log Insight-Appliance ist.

Hinweis In einer Umgebung, in der ein vRealize Operations Manager 6.1-Cluster mit einem konfigurierten Lastausgleichsdienst ausgeführt wird, können Sie die IP-Adresse des Lastausgleichsdiensts verwenden, falls verfügbar.

Vorgehensweise

1. Klicken Sie auf das Dropdown-Menüsymbol für die Konfiguration und wählen Sie **Verwaltung** aus.
2. Wählen Sie unter „Integration“ die Option **vRealize Operations Manager** aus.
3. Geben Sie die IP-Adresse oder den Hostnamen und die Anmeldedaten für die virtuelle Maschine der Benutzeroberfläche der vRealize Operations Manager-Instanz ein, und klicken Sie auf **Verbindung testen**.

   vRealize Log Insight verwendet Anmeldedaten, um Benachrichtigungsereignisse an vRealize Operations Manager zu senden. Die Verwendung von Anmeldedaten für das Dienstkonto wird empfohlen.
4. Wählen Sie im Bereich „vRealize Operations Manager“ **Integration von Warnungen aktivieren** aus.
5. Klicken Sie auf **Speichern**.

Weiter

- Die von vRealize Log Insight gesendeten Benachrichtigungsereignisse werden auf der vSphere-Benutzeroberfläche von vRealize Operations Manager nicht standardmäßig angezeigt. Navigieren Sie zu **Planung > Ereignisse** und klicken Sie auf **Benachrichtigungsereignisse zeigen**.
- Sie können Warnungsabfragen zum Senden von Benachrichtigungsereignissen an vRealize Operations Manager konfigurieren. Siehe Hinzufügen einer Warnungsabfrage in Log Insight, um Benachrichtigungsereignisse an vRealize Operations Manager zu senden.
- Sie können Warnungsabfragen zum Senden von Benachrichtigungsereignissen an vRealize Operations Manager konfigurieren. Weitere Informationen finden Sie unter dem Thema „Hinzufügen einer Warnungsabfrage in Log Insight, um Benachrichtigungsereignisse zu senden“ im vRealize Operations Manager *Log Insight-Benutzerhandbuch*.

vRealize Log Insight -Benachrichtigungsereignisse in vRealize Operations Manager

Sie können vRealize Log Insight konfigurieren, damit Benachrichtigungsereignisse an vRealize Operations Manager auf Basis der von Ihnen erstellten Warnungsabfragen gesendet werden.

Wenn Sie eine Benachrichtigungswarnung in vRealize Log Insight konfigurieren, wählen Sie eine Ressource in vRealize Operations Manager aus, die den Benachrichtigungsereignissen zugeordnet ist. Siehe Hinzufügen einer Warnungsabfrage in Log Insight, um Benachrichtigungsereignisse an vRealize Operations Manager zu senden.

Wenn Sie eine Benachrichtigungswarnung in vRealize Log Insight konfigurieren, wählen Sie eine Ressource in vRealize Operations Manager aus, die den Benachrichtigungsereignissen zugeordnet ist. Weitere Informationen finden Sie unter „Hinzufügen einer Warnungsabfrage in Log Insight, um Benachrichtigungsereignisse an vRealize Operations Manager zu senden“ im *Log Insight-Benutzerhandbuch*.

Der Speicherort der vRealize Log Insight-Benachrichtigungsereignisse hängt von der verwendeten Benutzeroberflächenversion von vRealize Operations Manager ab.

Tabelle 7-1. Bereiche der Benutzeroberfläche von vRealize Operations Manager , in denen Benachrichtigungsereignisse angezeigt werden

vRealize Operations Manager-Benutzeroberfläche	Bereiche, in denen vRealize Log Insight-Benachrichtigungsereignisse angezeigt werden
Benutzerdefinierte Benutzeroberfläche	■ Seite „Warnungen – Übersicht". ■ Alle Dashboards, in denen das Dashboard-Widget „Warnungen" angezeigt wird
vSphere-Benutzeroberfläche	■ Registerkarte **Ereignisse** unter der Registerkarte **Vorgänge** ■ Registerkarte **Ereignisse** unter der Registerkarte **Planung**

Der Name und die Beschreibung der Warnung, die Sie in vRealize Log Insight angegeben haben, werden in der Spalte „Warnungsinformationen" der Warnungsliste in vRealize Operations Manager angezeigt.

In der benutzerdefinierten Benutzeroberfläche ist die Spalte „Warnungsinformationen" standardmäßig nicht sichtbar. Sie können die Spalte „Warnungsinformationen" aktivieren, indem Sie das Dropdown-Menü in der Tabellenkopfzeile erweitern und das Kontrollkästchen **Warnungsinformationen** aktivieren.

Aktivieren der Active Directory-Integration von vRealize Log Insight und vRealize Operations Manager

Um vRealize Log Insight und vRealize Operations Manager unter Verwendung einer LDAP-Quelle zu integrieren, benötigen Sie den Namen der LDAP-Quelle in vRealize Operations Manager. In vRealize Log Insight müssen Sie sie mit Benutzer@Domäne@Quelle integrieren. Stellen Sie dabei sicher, dass der Benutzer, den Sie in vRealize Operations Manager erstellt haben, über die Berechtigungen zum Bearbeiten von Objekten in vRealize Operations Manager verfügt.

Sie benötigen Administratorzugriff sowohl auf vRealize Log Insight als auch auf vRealize Operations Manager, um die Integration durchzuführen.

Vorgehensweise

1 Rufen Sie in vRealize Operations Manager den Namen der LDAP-Quelle (SOURCE) auf, die Zugriff auf vRealize Operations Manager haben wird.

2 Stellen Sie sicher, dass der Benutzer über die entsprechenden Rechte zum Erstellen von Ressourcen und Beziehungen sowie über das Recht, Ressourcen zu löschen, verfügt.

3 (Optional) Um sicherzugehen, dass der Zugriff möglich ist, lassen Sie den Benutzer sich bei vRealize Operations Manager anmelden.

4 In vRealize Log Insight muss der Benutzer als BENUTZER@QUELLE angegeben werden. Wenn es sich bei dem Benutzer um einen UPN handelt (durch NAME@DOMÄNE zu erkennen), muss der Benutzer in vRealize Log Insight als BENUTZER@DOMÄNE@QUELLE angegeben werden.

Hinzufügen einer Suchdomäne

Sie können eine Suchdomäne hinzufügen, um den vRealize Operations Manager-Inventarabgleich zu optimieren.

Durch das Hinzufügen einer Suchdomäne wird der Abgleich, wenn die Beschriftungs- und Suchdomäne einer virtuellen Maschine in Bezug auf die IP-Adresse des Hosts aufgelöst wird, welcher Protokollmeldungen an vRealize Log Insight sendet, verbessert. Beispiel: Wenn Sie über eine virtuelle Maschine mit der Bezeichnung linux_01 in vRealize Operations Manager verfügen und wenn der Hostname linux_01.company.com in 192.168.10.10 aufgelöst wird, kann vRealize Log Insight durch das Hinzufügen einer Suchdomäne diese Ressource erkennen und abgleichen.

Voraussetzungen

- Stellen Sie sicher, dass Sie über die Root-Benutzer-Anmeldedaten verfügen, um sich bei der virtuellen vRealize Log Insight-Appliance anzumelden. Siehe „Konfigurieren des SSH-Root-Kennworts für die virtuelle Log Insight-Appliance“, auf Seite 16.
- Um SSH-Verbindungen zu aktivieren, überprüfen Sie zunächst, ob der TCP-Port 22 geöffnet ist.

Vorgehensweise

1 Stellen Sie eine SSH-Verbindung zur virtuellen vRealize Log Insight-Appliance her und melden Sie sich als Root-Benutzer an.

2 Öffnen Sie `/etc/resolv.conf`.

3 Geben Sie Ihre Suchdomäne ein. Beispiel: `search company.com`.

4 Speichern und schließen Sie die Datei.

Installieren des vRealize Log Insight -Adapters in der Standalone-Version von vRealize Operations Manager

Sie können den vRealize Log Insight-Adapter in der Standalone-Version von vRealize Operations Manager installieren, um den kontextbezogenen Start zu aktivieren.

Der vRealize Log Insight-Adapter liefert vRealize Operations Manager die notwendigen Informationen, um vRealize Log Insight zu starten. Dieser Adapter sammelt keine Daten.

Der vRealize Log Insight-Adapter wird als Teil der vRealize Operations Manager 5.7.1-vApp, nicht jedoch als Teil der Standalone-Version von vRealize Operations Manager installiert. Daher müssen Sie für die Standalone-Version den vRealize Log Insight-Adapter manuell installieren.

Der vRealize Log Insight-Adapter ist als Teil von vRealize Operations Manager 5.7.2 und 5.8 installiert.

VMware verteilt den vRealize Log Insight-Adapter als `.tgz`-Archiv, das die Installationsprogramme für Windows und Linux enthält.

Voraussetzungen

- Laden Sie die Management Pack-Installationsdatei von https://solutionexchange.vmware.com/store/category_groups/cloud-management herunter. Sie können die TGZ-Datei über die Registerkarte „Ressourcen“ der Management-Pack-Seite herunterladen.
- Notieren Sie sich die Build-Nummer im Namen TGZ-Datei. Die Build-Nummer wird nach dem Namen des Management Packs angezeigt, zum Beispiel *`managementpack_name-buildnumber`*`.tgz`.
- Stellen Sie sicher, dass Sie Zugriff auf den Server haben, auf dem vRealize Operations Managerausgeführt wird, und dass Sie über die entsprechenden Berechtigungen verfügen, um Software auf dem Server installieren.
- Vergewissern Sie sich, dass die Version von vRealize Operations Manager 5.7.1 oder höher ist.
- Sie müssen die IP-Adresse oder den Hostnamen der Zielinstanz von vRealize Operations Manager kennen.

- Vergewissern Sie sich je nach Art Ihrer Lizenz von vRealize Operations Manager, dass Sie über die minimal erforderlichen Anmeldedaten verfügen.

vRealize Operations Manager-Lizenz	Minimal erforderliche Anmeldedaten
Standard	Standard-Admin-Anmeldedaten
Advanced oder Enterprise	Anmeldedaten für Anwender mit Leseberechtigung

Hinweis vRealize Log Insight bietet keine Unterstützung für die Active Directory-Integration mit vRealize Operations Manager.

Vorgehensweise

1 Öffnen Sie die TGZ-Datei und extrahieren Sie die TAR-Datei an einem temporären Speicherort auf Ihrem vRealize Operations Manager-Server.

2 Öffnen Sie im temporären Ordner die TAR-Datei und extrahieren und führen Sie das Installationsprogramm für Ihre Betriebssystemplattform aus.

3 Melden Sie sich bei vRealize Operations Manager als Administrator an.

4 Wählen Sie **Admin > Support** aus.

5 Suchen Sie auf der Registerkarte **Info** den Bereich „Adapterinformationen“ und klicken Sie auf das Symbol **Beschreiben** ( ).

Das **Describe**-Symbol befindet sich oben rechts im Bereich „Adapterinformationen“.

6 Klicken Sie auf **Ja**, um den Describe-Vorgang zu starten.

7 Überprüfen Sie, ob die Build-Nummer in der Spalte „Adapterversion“ für das Management Pack mit der Build-Nummer in der TGZ-Datei übereinstimmt, die Sie heruntergeladen haben.

Weiter

Aktivieren Sie nach der Installation des Adapters den kontextbezogenen Start über die Verwaltungs-Web-Benutzeroberfläche von vRealize Log Insight.

Weitere Informationen hierzu finden Sie unter „Aktivieren des kontextbezogenen Starts für vRealize Log Insight in vRealize Operations Manager“, auf Seite 84.

Weitere Informationen finden Sie unter *Aktivieren des kontextbezogenen Starts für vRealize Log Insight in vRealize Operations Manager* im *Log Insight-Administratorhandbuch*.

vRealize Operations Manager -Inhaltspaket für vRealize Log Insight

Das vRealize Operations Manager-Inhaltspaket für vRealize Log Insight enthält Dashboards, extrahierte Felder, gespeicherte Abfragen und Warnungen, die zur Analyse aller von einer vRealize Operations Manager-Instanz umgeleiteten Protokolle verwendet werden.

Das vRealize Operations Manager-Inhaltspaket bietet die Möglichkeit, alle von einer vRealize Operations Manager-Instanz umgeleiteten Protokolle zu analysieren. Das Inhaltspaket enthält Dashboards, Abfragen und Warnungen, die dem vRealize Operations Manager-Administrator die Diagnose und Fehlerbehebung ermöglichen sollen. Die Dashboards sind zur besseren Verwaltbarkeit nach den Hauptkomponenten von vRealize Operations Manager wie Analyse, Benutzeroberfläche und Adapter gruppiert. Sie können verschiedene Alarme für das Versenden von Benachrichtigungsereignissen in vRealize Operations Manager und von E-Mails an Administratoren aktivieren.

Hinweis Für das Inhaltspaket von vRealize Operations Manager sind vRealize Log Insight Version 1.5 und vRealize Operations Manager Version 5.8 erforderlich.

Das Inhaltspaket von vRealize Operations Manager kann über https://solutionexchange.vmware.com/store/loginsight?src=Product_Product_LogInsight_YES_US heruntergeladen werden.

Siehe Arbeiten mit Inhaltspaketen.

Siehe unter „Arbeiten mit Inhaltspaketen“ im *Log Insight-Benutzerhandbuch*.

Aktivieren des kontextbezogenen Starts für vRealize Log Insight in vRealize Operations Manager

Sie können vRealize Operations Manager so konfigurieren, dass mit vRealize Log Insight in Zusammenhang stehende Menüelemente angezeigt werden und vRealize Log Insight mit einer objektspezifischen Abfrage gestartet wird.

Sie können vRealize Log Insight in vRealize Operations Manager vApp und vRealize Operations Manager Installable integrieren. Die Integration in die Installable-Version erfordert zusätzliche Änderungen an der Konfiguration von vRealize Operations Manager. Informationen zur Konfiguration von vRealize Operations Manager Installable zur Integration in vRealize Log Insightfinden Sie in der Anleitung *Erste Schritte für Log Insight*.

Wichtig Eine Instanz von vRealize Operations Manager unterstützt den kontextbezogenen Start für nur eine Instanz von vRealize Log Insight. Da vRealize Log Insight nicht überprüft, ob bei vRealize Operations Manager bereits andere Instanzen registriert sind, könnten Sie die Einstellungen eines anderen Benutzers außer Kraft setzen.

Voraussetzungen

- Vergewissern Sie sich, dass Sie bei der Web-Benutzeroberfläche von vRealize Log Insightals Benutzer mit der Berechtigung **Admin bearbeiten** angemeldet sind. Das URL-Format lautet https://*log-insight-host*, wobei *log-insight-host* die IP-Adresse oder der Hostname der virtuellen vRealize Log Insight-Appliance ist.
- Sie müssen die IP-Adresse oder den Hostnamen der Zielinstanz von vRealize Operations Manager kennen.
- Vergewissern Sie sich je nach Art Ihrer Lizenz von vRealize Operations Manager, dass Sie über die minimal erforderlichen Anmeldedaten verfügen.

vRealize Operations Manager-Lizenz	Minimal erforderliche Anmeldedaten
Standard	Standard-Admin-Anmeldedaten
Advanced oder Enterprise	Anmeldedaten für Anwender mit Leseberechtigung

  Hinweis vRealize Log Insight bietet keine Unterstützung für die Active Directory-Integration mit vRealize Operations Manager.

- Vergewissern Sie sich, dass die Version von vRealize Operations Manager 5.7.1 oder höher ist.

  Hinweis vRealize Log Insight überprüft die Zielversion von vRealize Operations Manager nicht und ermöglicht es Ihnen, fortzufahren. Jedoch ist vRealize Operations Manager 5.7.1 oder höher erforderlich, damit die Verknüpfung zurück zu vRealize Log Insight funktioniert und die Warnung geöffnet wird, die das Benachrichtigungsereignis generiert hat.

  Weitere Informationen zu unterstützten Produktversionen finden Sie unter Produktkompatibilität.

Vorgehensweise

1 Klicken Sie auf das Dropdown-Menüsymbol für die Konfiguration und wählen Sie **Verwaltung** aus.

2 Wählen Sie unter „Integration“ die Option **vRealize Operations Manager** aus.

3 Geben Sie die IP-Adresse oder den Host- Namen sowie die Anmeldedaten für die virtuelle Maschine der Benutzeroberfläche der vRealize Operations Manager-vApp ein, und klicken Sie auf **Verbindung testen**.

Hinweis Sie müssen die Benutzeranmeldedaten eines vRealize Operations Manager-Administrators eingeben.

4 Klicken Sie auf **Speichern**.

vRealize Log Insight konfiguriert die vRealize Operations Manager-Instanz. Dieser Vorgang kann einige Minuten dauern.

Es werden mit vRealize Log Insight in Zusammenhang stehende Elemente in den Menüs von vRealize Operations Manager angezeigt.

Weiter

Starten Sie eine vRealize Log Insight-Abfrage aus der vRealize Operations Manager-Instanz. Siehe „Kontextbezogener Start von vRealize Log Insight“, auf Seite 85.

Kontextbezogener Start von vRealize Log Insight

Sie können vRealize Operations Manager 5.7.1 oder höher konfigurieren, um Aktionen in Verbindung mit vRealize Log Insight auszulösen.

Wenn Sie den kontextbezogenen Start für vRealize Log Insight aktivieren, wird eine vRealize Log Insight-Ressource unter dem HTTP-Post-Adapter in vRealize Operations Manager erstellt. Der Ressourcenbezeichner enthält die IP-Adresse der vRealize Log Insight-Instanz und wird von vRealize Operations Manager zum Öffnen von vRealize Log Insight verwendet.

Kontextbezogener Start in der vSphere-Benutzeroberfläche von vRealize Operations Manager

Die kontextbezogenen Startoptionen in Verbindung mit vRealize Log Insight werden im Dropdown-Menü **Aktionen** der vSphere-Benutzeroberfläche angezeigt. Sie können diese Menüelemente verwenden, um vRealize Log Insight zu öffnen und um Protokollereignisse von einem Objekt in vRealize Operations Manager zu suchen.

Welche kontextbezogene Startaktion verfügbar ist, hängt vom Objekt ab, das Sie im vRealize Operations Manager-Bestand auswählen. Der Zeitraum der Abfragen ist auf 60 Minuten vor dem Klicken auf eine kontextbezogene Startoption begrenzt.

Tabelle 7-2. Objekte in der vSphere-Benutzeroberfläche von vRealize Operations Manager und deren entsprechende kontextbezogene Startoptionen und -aktionen

In vRealize Operations Manager ausgewählte Objekte	Kontextbezogene Startoption im Dropdown-Menü Aktionen	Aktion in vRealize Operations Manager	Aktion in vRealize Log Insight
World	**Öffnen von vRealize Log Insight**	Öffnet vRealize Log Insight.	vRealize Log Insight zeigt die Registerkarte **Interaktive Analyse** an.
vCenter Server	**Öffnen von vRealize Log Insight**	Öffnet vRealize Log Insight.	vRealize Log Insight zeigt die Registerkarte **Interaktive Analyse** an.

Tabelle 7-2. Objekte in der vSphere-Benutzeroberfläche von vRealize Operations Manager und deren entsprechende kontextbezogene Startoptionen und -aktionen (Fortsetzung)

In vRealize Operations Manager ausgewählte Objekte	Kontextbezogene Startoption im Dropdown-Menü Aktionen	Aktion in vRealize Operations Manager	Aktion in vRealize Log Insight
Datencenter	**Suchen nach Protokollen in vRealize Log Insight**	Öffnet vRealize Log Insight und übergibt die Ressourcennamen aller Hostsysteme unter dem ausgewählten Datencenter-Objekt.	vRealize Log Insight zeigt die Registerkarte **Interaktive Analyse** an und führt eine Abfrage durch, um Protokollereignisse zu finden, die Hostnamen des Datencenters enthalten.
Cluster	**Suchen nach Protokollen in vRealize Log Insight**	Öffnet vRealize Log Insight und übergibt die Ressourcennamen aller Hostsysteme unter dem ausgewählten Clusterobjekt.	vRealize Log Insight zeigt die Registerkarte **Interaktive Analyse** an und führt eine Abfrage durch, um Protokollereignisse zu finden, die Hostnamen des Clusters enthalten.
Hostsystem	**Suchen nach Protokollen in vRealize Log Insight**	Öffnet vRealize Log Insight und übergibt den Ressourcennamen des ausgewählten Hostobjekts.	vRealize Log Insight zeigt die Registerkarte **Interaktive Analyse** an und führt eine Abfrage durch, um Protokollereignisse zu finden, die den Namen des ausgewählten Hostsystems enthalten.
Virtuelle Maschine	**Suchen nach Protokollen in vRealize Log Insight**	Öffnet vRealize Log Insight und übergibt die IP-Adresse der ausgewählten virtuellen Maschine und den Ressourcennamen des verbundenen Hostsystems.	vRealize Log Insight zeigt die Registerkarte **Interaktive Analyse** an und führt eine Abfrage durch, um Protokollereignisse zu finden, die die IP-Adresse der virtuellen Maschine und den Namen des Hosts, auf dem sich die virtuelle Maschine befindet, enthalten.

Wenn Sie auf der Registerkarte **Warnungen** eine Warnung auswählen und dann im Kontextmenü auf **Protokolle in Log Insight suchen** klicken, wird der Zeitraum auf eine Stunde vor dem Auslösen der Warnung begrenzt. Wenn beispielsweise eine Warnung um 14:00 Uhr ausgelöst wurde, zeigt die Abfrage in vRealize Log Insight alle Protokollmeldungen an, die sich zwischen 13:00 und 14:00 Uhr ereigneten. Dies hilft Ihnen, Ereignisse zu identifizieren, die die Warnung ausgelöst haben könnten.

Sie können vRealize Log Insight über Metrikdiagramme in vRealize Operations Manager öffnen. Der Zeitraum der Abfrage, die von vRealize Log Insight ausgeführt wird, entspricht dem Zeitraum des Metrikdiagramms.

Hinweis Die Zeiten, die in vRealize Log Insight und den Metrikdiagrammen in vRealize Operations Manager angezeigt werden, können unterschiedlich sein, wenn die Zeiteinstellung der virtuellen Appliances unterschiedlich ist.

Kontextbezogener Start in der benutzerdefinierten Benutzeroberfläche von vRealize Operations Manager

Das kontextbezogene Startsymbol wird zwar auf mehreren Seiten der benutzerdefinierten Benutzeroberfläche angezeigt, Sie können jedoch vRealize Log Insight nur von den Seiten aus starten, auf denen die vRealize Log Insight-Benachrichtigungsereignisse angezeigt werden:

- Seite „Warnungen – Überblick".
- Seite „Warnung – Zusammenfassung" einer vRealize Log Insight-Benachrichtigungswarnung.

- Widgets „Warnungen“ auf Ihren Dashboards, wenn eine vRealize Log Insight-Benachrichtigungswarnung ausgewählt ist.

Wenn Sie in der benutzerdefinierten Benutzeroberfläche ein vRealize Log Insight-Benachrichtigungsereignis auswählen, können Sie unter zwei kontextbezogenen Startaktionen wählen.

Tabelle 7-3. Kontextbezogene Startoptionen und -aktionen in der benutzerdefinierten Benutzeroberfläche von vRealize Operations Manager

Kontextbezogene Startoption in vRealize Operations Manager	Aktion in vRealize Operations Manager	Aktion in vRealize Log Insight
Öffnen von vRealize Log Insight	Öffnet vRealize Log Insight.	vRealize Log Insight zeigt die Registerkarte **Dashboards** an und lädt das Dashboard „vSphere-Übersicht“.
Suchen nach Protokollen in vRealize Log Insight	Öffnet vRealize Log Insight und übergibt den Bezeichner der Abfrage, die das Benachrichtigungsereignis ausgelöst hat.	vRealize Log Insight zeigt die Registerkarte **Interaktive Analyse** an und führt die Abfrage durch, die das Benachrichtigungsereignis ausgelöst hat.

Wenn Sie eine Warnung auswählen, die nicht von vRealize Log Insight stammt, enthält das kontextbezogene Startmenü das Menüelement **VM- und Hostprotokolle in vRealize Log Insight suchen**. Wenn Sie dieses Menüelement wählen, öffnet vRealize Operations Manager vRealize Log Insight und übergibt die Bezeichner des Objekts, das die Warnung ausgelöst hat. vRealize Log Insight verwendet die Ressourcenbezeichner, um eine Suche in den verfügbaren Protokollereignissen durchzuführen.

Deaktivieren des kontextbezogenen Starts für vRealize Log Insight in vRealize Operations Manager

Sie können den vRealize Log Insight-Adapter von der vRealize Operations Manager-Instanz deinstallieren, um mit vRealize Log Insight verbundene Menüelemente von der Benutzeroberfläche von vRealize Operations Manager zu entfernen.

Über die Benutzeroberfläche von vRealize Log Insight für Administratoren können Sie den kontextbezogenen Start deaktivieren. Wenn Sie nicht auf vRealize Log Insight zugreifen können oder die vRealize Log Insight-Instanz gelöscht wird, bevor die Verbindung mit vRealize Operations Manager deaktiviert wird, können Sie die Registrierung von vRealize Log Insight über die Administrations-Benutzeroberfläche von vRealize Operations Manager aufheben. Weitere diesbezügliche Informationen finden Sie in der Hilfe des Verwaltungsportals von vRealize Operations Manager.

Vorsicht Eine Instanz von vRealize Operations Manager unterstützt den kontextbezogenen Start für nur eine Instanz von vRealize Log Insight. Wenn eine andere vRealize Log Insight-Instanz registriert wurde, nachdem Sie die Instanz, die Sie deaktivieren möchten, registriert haben, setzt die zweite Instanz die Einstellungen der ersten außer Kraft, ohne Sie zu benachrichtigen.

Voraussetzungen

- Vergewissern Sie sich, dass Sie bei der Web-Benutzeroberfläche von vRealize Log Insightals Benutzer mit der Berechtigung **Admin bearbeiten** angemeldet sind. Das URL-Format lautet https://*log-insight-host*, wobei *log-insight-host* die IP-Adresse oder der Hostname der virtuellen vRealize Log Insight-Appliance ist.

Vorgehensweise

1 Klicken Sie auf das Dropdown-Menüsymbol für die Konfiguration und wählen Sie **Verwaltung** aus.

2 Wählen Sie unter „Integration“ die Option **vRealize Operations Manager** aus.

3 Deaktivieren Sie das Kontrollkästchen **Kontextbezogenen Start aktivieren**.

4 Klicken Sie auf **Speichern**.

vRealize Log Insight konfiguriert die vRealize Operations Manager-Instanz so, dass diese den vRealize Log Insight-Adapter entfernt. Dieser Vorgang kann einige Minuten dauern.

Entfernen des vRealize Log Insight -Adapters aus einer vRealize Operations Manager -Instanz

Wenn Sie den kontextbezogenen Start für eine vRealize Operations Manager-Instanz aktivieren, erstellt vRealize Log Insight eine Instanz des vRealize Log Insight-Adapters in der vRealize Operations Manager-Instanz.

Die Instanz des Adapters bleibt in der vRealize Operations Manager-Instanz, wenn Sie vRealize Log Insight deinstallieren. Dadurch werden die Elemente des Menüs für den kontextbezogenen Start weiterhin im Menü „Aktionen“ angezeigt und verweisen auf eine vRealize Log Insight-Instanz, die nicht mehr existiert.

Um den kontextbezogenen Start in vRealize Operations Manager zu deaktivieren, müssen Sie den vRealize Log Insight-Adapter aus der vRealize Operations Manager-Instanz entfernen.

Sie können das Befehlszeilendienstprogramm cURL verwenden, um REST-Anrufe an vRealize Operations Manager zu senden.

Voraussetzungen

- Überprüfen Sie, ob cURL auf Ihrem System installiert ist.
- Sie müssen die IP-Adresse oder den Hostnamen der Zielinstanz von vRealize Operations Manager kennen.
- Vergewissern Sie sich je nach Art Ihrer Lizenz von vRealize Operations Manager, dass Sie über die minimal erforderlichen Anmeldedaten verfügen.

vRealize Operations Manager-Lizenz	Minimal erforderliche Anmeldedaten
Standard	Standard-Admin-Anmeldedaten
Advanced oder Enterprise	Anmeldedaten für Anwender mit Leseberechtigung

Hinweis vRealize Log Insight bietet keine Unterstützung für die Active Directory-Integration mit vRealize Operations Manager.

Vorgehensweise

1 Führen Sie in cURL die folgende Abfrage für die virtuelle vRealize Operations Manager-Appliance aus, um den vRealize Log Insight-Adapter zu finden.

```
curl –k ––user Admin–Benutzername:Kennwort
https://URL:443/HttpPostAdapter/OpenAPIServlet –d
"action=getRelationships&resourceName=Log Insight
Server&adapterKindKey=LogInsight&resourceKindKey=LogInsightLogServer&
getChildren=true&getParents=false"
```

Dabei sind *Admin-Benutzername* und *Kennwort* die Anmeldedaten des Administrators und *URL* die IP-Adresse der vRealize Operations Manager-Instanz.

Die Abfrage liefert ein Ergebnis in folgendem Format:

```
resourceName=Log Insight Server&adapterKindKey=LogInsight&resourceKindKey=LogInsightLogServer

Parents:
```

```
Children:
resourceName=Log Insight Server<Log Insight-Pfad>&
adapterKindKey=LogInsight&
resourceKindKey=LogInsightLogServerHost&
identifiers=HOST::<Log Insight-Pfad>
```

Dabei ist *Log Insight-Pfad* der HOST-Wert des untergeordneten Objekts der abgefragten Ressource. Sie können diesen Wert im Befehl zum Entfernen der Adapterinstanz verwenden.

2 Führen Sie den folgenden Befehl aus, um den vRealize Log Insight-Adapter zu entfernen:

```
curl -k --user <Admin-Benutzername>:<Kennwort> https://<URL>:443/HttpPostAdapter/OpenAPIServlet -d
"action=addRemoveParentChildRelationship&parentResource=Log Insight Server&adapterKindKey=Lo-
gInsight&
resourceKindKey=LogInsightLogServer&addFlag=false&
childResources=Log Insight Server<Log Insight-Pfad>,LogInsight,LogInsightLogServer-
Host,HOST::<Log Insight-Pfad>"
```

Dabei sind *Admin-Benutzername* und *Kennwort* die Anmeldedaten des Administrators, *URL* die IP-Adresse der vRealize Operations Manager-Instanz und *Log Insight-Pfad* der Hostspeicherort der untergeordneten Ressource der Beziehung, die Sie entfernen möchten.

Elemente des kontextbezogenen Starts von vRealize Log Insight werden aus den Menüs in vRealize Operations Manager entfernt. Weitere Informationen zum kontextbezogenen Start finden Sie unter *Kontextbezogener Start von vRealize Log Insight* in der produktbezogenen Hilfe von vRealize Log Insight.

Sichern, Wiederherstellen und die Notfallwiederherstellung 8

Halten Sie sich an die Best Practices für das Sichern, Wiederherstellen und für die Notfallwiederherstellung, um kostspielige Datencenter-Ausfälle zu vermeiden.

Dieses Kapitel behandelt die folgenden Themen:

- „Best Practices für das Sichern, Wiederherstellen und für die Notfallwiederherstellung“, auf Seite 91
- „Allgemeine Richtlinien“, auf Seite 92
- „Allgemeine Empfehlungen“, auf Seite 93
- „Richtlinien für das Sichern und Replizieren“, auf Seite 93
- „Richtlinien für die Wiederherstellung und die Notfallwiederherstellung“, auf Seite 95
- „Richtlinien für Konfigurationsänderungen nach der Wiederherstellung“, auf Seite 96

Best Practices für das Sichern, Wiederherstellen und für die Notfallwiederherstellung

Halten Sie sich an die Best Practices für das Sichern, Wiederherstellen und für die Notfallwiederherstellung, um kostspielige Datencenter-Ausfälle zu vermeiden.

In diesem Kapitel werden Richtlinien für die Best Practices für das Sichern, Wiederherstellen und für die Notfallwiederherstellung der folgenden vRealize Log Insight-Versionen und -Komponenten beschrieben.

Version von vRealize Log Insight	Komponenten
3.0 GA	Masterknoten, Worker-Knoten, Agent, Forwarder
2.5 GA	Masterknoten, Worker-Knoten, Agent, Forwarder

In diesem Kapitel werden die folgenden Tools und Produkte nicht beschrieben.

- In diesem Kapitel werden keine Tool-spezifischen Schritte für das Sichern, Wiederherstellen und für die Notfallwiederherstellung behandelt. Tool- und produktspezifische Informationen finden Sie in der Produktdokumentation.
- Informationen zu den Best Practices für VDP, SRM und NetBackup im Zusammenhang mit bestimmten Tools finden Sie im Whitepaper „VMware vCloud Suite Best Practices“.
- In diesem Kapitel werden keine Richtlinien für das Sichern, Wiederherstellen und für die Notfallwiederherstellung der folgenden Produkte beschrieben, die mit vRealize Log Insight integriert werden können.
  - vRealize Operations Manager

- VMware vSphere-Server
- ESXi-Hosts
- Andere Produkte, die mit vRealize Log Insight integriert werden können

Allgemeine Richtlinien

Folgen Sie diesen Richtlinien für Sicherungsvorgänge und eine einfachere Wiederherstellung von vRealize Log Insight 3.0 GA- und 2.5 GA-Clustern in einer neuen Umgebung

vRealize Log Insight 3.0 GA und 2.5 GA unterstützen die folgenden Best Practices und Richtlinien.

- Verwenden Sie statische IP-Adressen für alle Knoten in einem vRealize Log Insight-Cluster.
  - Durch die Verwendung von statischen IP-Adressen müssen Sie die IP-Adressen von vRealize Log Insight-Clusterknoten nicht jedes Mal ändern, wenn sich die IP-Adresse eines vRealize Log Insight-Knotens ändert.
  - vRealize Log Insight nimmt alle Knoten-IP-Adressen in jede Clusterknoten-Konfigurationsdatei unter `/storage/core/loginsight/config/loginsight-config.xml#<n>` auf, wobei `<n>` die höchste Nummer ist.
  - Alle Produkte, die mit vRealize Log Insight integriert sind, um ihre Protokolle weiterzuleiten (z. B. ESXi, vSphere und vRealize Operations), verwenden den FQDN oder die IP-Adresse des Cluster-Masterknotens (oder des Lastausgleichsdiensts, sofern konfiguriert) als Syslog-Ziel. Statische IP-Adressen reduzieren das Risiko, die Syslog-Ziel-IP-Adresse mehrerer Sites ständig aktualisieren zu müssen.
- Verwenden Sie einen FQDN für alle Knoten im vRealize Log Insight-Cluster.
  - Ein vollständig auflösbarer FQDN ist für den Masterknoten (Lastausgleichsdienst, falls verwendet) erforderlich. Andernfalls können die ESXi-Hosts die Syslog-Meldungen nicht an vRealize Log Insight oder ein Remote-Ziel weiterleiten.
  - Durch die Verwendung eines FQDN sparen Sie Zeit bei Konfigurationsänderungen nach der Wiederherstellung, vorausgesetzt, derselbe FQDN kann auf der Wiederherstellungs-Site aufgelöst werden.
  - vRealize Log Insight verwendet FQDN-Hostnamen, sofern vorhanden, an Stelle von IP-Adressen für Systemwarnungen.
  - Vorausgesetzt, dass sich nach Sicherungs-/Wiederherstellungs- und Notfallwiederherstellungsvorgängen nur die zugrunde liegenden IP-Adressen ändern, entfällt bei der Verwendung von FQDN die Notwendigkeit, die Syslog-Zieladresse (Masterknoten-FQDN oder FQDN des internen Lastausgleichsdiensts) auf allen externen Geräten zu ändern, die Protokollmeldungen an den vRealize Log Insight-Cluster weiterleiten.
  - Bei vRealize Log Insight 2.5 GA müssen Sie die Konfigurationsdatei aktualisieren (unter `/storage/core/loginsight/config/loginsight-config.xml#<n>`, wobei `<n>` die höchste Nummer ist), um die IP-Adresse des Worker-Knotens durch die neue, für die wiederhergestellten Knoten verwendete IP-Adresse zu ersetzen, da in der Konfigurationsdatei der FQDN nicht für die Worker-Knotenadressen verwendet wird. Sie müssen diese Änderung nur auf dem Masterknoten vornehmen. Die Änderungen werden mittels Synchronisierung an alle Worker-Knoten weitergegeben.
- Bei Anforderungen zum Beitreten von einem vRealize Log Insight-Worker-Knoten sollte der FQDN des vRealize Log Insight-Masterknotens verwendet werden.
  - Ab vRealize Log Insight 2.5 basiert der Wert für den Host des Masterknotens in der Konfigurationsdatei auf jedem Knoten (unter `/storage/core/loginsight/config/loginsight-config.xml#<n>`) auf dem Wert, der vom ersten Worker-Knoten verwendet wird, der eine Anforderung zum Beitreten sendet. Wenn für die Anforderung zum Beitreten der FQDN des Masterknotens verwendet

wird, können nach der Notfallwiederherstellung keine manuellen Änderungen am Wert für den Host des Masterknotens vorgenommen werden. Anderenfalls kann der Worker-Knoten dem Masterknoten erst dann erneut beitreten, wenn in den Konfigurationsdateien auf allen wiederhergestellten Clusterknoten der Hostname des Masterknotens aktualisiert wurde.

- Geben Sie statische IP-Adressen sowie optionale virtuelle IP-Adressen für den Lastausgleichsdienst an.
  - Bei der Konfiguration eines integrierten Lastausgleichsdiensts geben Sie den (optionalen) FQDN für die virtuelle IP-Adresse an. Dadurch kann vRealize Log Insight auf den FQDN zurückgreifen, wenn aus irgendeinem Grund eine IP-Adresse nicht erreichbar ist.

Allgemeine Empfehlungen

Halten Sie sich an diese Empfehlungen für Sicherungsvorgänge.

Die folgenden Empfehlungen können Ihnen beim Vorbereiten von Sicherungs- und Wiederherstellungsvorgängen helfen.

- Führen Sie einen Testlauf der Sicherungs-, Wiederherstellungs- und Notfallwiederherstellungsvorgänge in einer Test- oder Staging-Umgebung durch, bevor Sie diese Vorgänge live durchführen.
- Ereignisweiterleitungen – Je nach Kundenanforderungen kann es eine einzige oder mehrere vRealize Log Insight-Ereignisweiterleitungen geben. Darüber hinaus können die Ereignisweiterleitungen als Standalone-Knoten oder als Cluster installiert werden. Zum Zwecke der Sicherungs-, Wiederherstellungs und Notfallwiederherstellungsvorgänge sind vRealize Log Insight-Ereignisweiterleitungen identisch mit den primären vRealize Log Insight-Clusterknoten, sodass die gleichen, für den vRealize Log Insight-Hauptcluster empfohlenen Sicherungs-, Wiederherstellungs und Notfallwiederherstellungsschritte auch für die Ereignisweiterleitungen gelten.
- Führen Sie eine vollständige Sicherung des gesamten vRealize Log Insight-Clusters durch und verlassen Sie sich nicht auf automatische Vorgänge zur Sicherung einzelner Dateien und Konfigurationen.
- Stellen Sie sicher, dass die empfohlene Menge an Ressourcen für den vRealize Log Insight-Cluster sowie die Sicherungs-, Wiederherstellungs- und Notfallwiederherstellungs-Tools zugeteilt wurden, gemäß den Empfehlungen in der Dokumentation für die einzelnen Sicherungs-, Wiederherstellungs- und Notfallwiederherstellungs-Tools.
- Stellen Sie sicher, dass die spezifischen empfohlenen Vorgehensweisen für die Tools eingehalten werden, gemäß den Empfehlungen in der Dokumentation für die einzelnen Sicherungs-, Wiederherstellungs- und Notfallwiederherstellungs-Tools.
- Verwenden Sie zusätzliche Tools, die spezielle Funktionen und Konfigurationen zum Unterstützen von Sicherungen, Wiederherstellungen und Notfallwiederherstellungen von virtuellen Maschinen bieten, die mithilfe von VMware-Produkten bereitgestellt wurden.
- Bevor Sie Sicherungs-, Wiederherstellungs- und Notfallwiederherstellungsvorgänge durchführen, stellen Sie sicher, dass alle Fehlerkorrekturen implementiert und die Ursachen von Warnungen und Fehlern behoben wurden. Sicherungs-, Wiederherstellungs- und Notfallwiederherstellungs-Tools bieten in der Regel visuelle Validierungen und Schritte, um sicherzugehen, dass die Sicherungs-, Wiederherstellungs- und Notfallwiederherstellungskonfigurationen ordnungsgemäß erstellt wurden.

Richtlinien für das Sichern und Replizieren

Bestimmte Richtlinien für das Sichern und Replizieren bieten zusätzliche Best Practices.

- Bestehende Probleme – Bevor Sie die Sicherungs- und Wiederherstellungsvorgänge durchführen, stellen Sie sicher, dass es keine Konfigurationsprobleme auf den Quell- und Ziel-Sites gibt.

- Zuteilung von vRealize Log Insight-Clusterressourcen – Bei vRealize Log Insight-Konfigurationen mit angemessenen Ingestions- und Abfrageauslastungen ist es möglich, dass während Sicherungs- und Replizierungsvorgängen die Arbeitsspeicher- und Swap-Nutzung fast 100 % erreicht. Da dies in einer Live-Umgebung erfolgt, ist die Arbeitsspeicherspitze zum Teil auf die vRealize Log Insight-Clusternutzung selbst zurückzuführen. Es ist auch möglich, dass die geplanten Sicherungs- und Replizierungsvorgänge erheblich zur Arbeitsspeicherspitze beitragen.
  - In einigen Fällen wurden Worker-Knoten kurzzeitig für ein bis drei Minuten getrennt, bevor sie wieder dem Masterknoten beitraten. Die Vermutung liegt nahe, dass dies aufgrund des hohen Arbeitsspeicherverbrauchs erfolgt.
  - So sorgen Sie für eine Reduzierung der Arbeitsspeicherdrosselung auf Log Insight-Knoten:
    - Teilen Sie zusätzlichen Arbeitsspeicher über die von vRealize Log Insight empfohlenen Konfigurationen hinaus zu und/oder
    - Planen Sie die wiederkehrenden Sicherungsvorgänge zu Zeiten außerhalb der Spitzenzeiten.
  - Obwohl CPU-Spitzen auftreten können, ist der Arbeitsspeicher oft das Hauptproblem.
- Snapshots stillgelegter Maschinen – vRealize Log Insight unterstützt keine Snapshots von stillgelegten Maschinen. Wenn Sie Tools für das Sichern, das Wiederherstellen oder die Notfallwiederherstellung verwenden, die Snapshots stillgelegter Maschinen unterstützen, achten Sie darauf, dass Sie das Stilllegen deaktivieren, bevor Sie das Sichern aktivieren.
- Ereignisweiterleitung – Aktivieren Sie die regelmäßige Sicherung und/oder Replizierung von vRealize Log Insight-Ereignisweiterleitungen unter Verwendung der gleichen Verfahren wie bei den vRealize Log Insight-Servern.
- Unterstützung von Agenten – vRealize Log Insight-Server unterstützen Linux- und Windows-Agenten
  - Wenn die Agentenkonfiguration serverseitig erstellt wird, ist keine separate Sicherung des Agentenknotens erforderlich.
  - Wenn Sie die Agentenknoten für andere Aufgaben als das Installieren der Agent-Software verwenden und diese Knoten vollständig gesichert werden müssen, führen Sie die Datensicherung so durch, als würden Sie eine virtuelle Maschine sichern.
  - Wenn die Agentenkonfiguration clientseitig (auf den Agenten) durchgeführt wird und die Agentenknoten nur verwendet werden, um die vRealize Log Insight-Agent-Software auf ihnen zu installieren, reicht es, die Agentenkonfigurationsdatei zu sichern. Sichern Sie die Datei `liagent.ini` und ersetzen Sie die Datei auf dem wiederhergestellten Agenten oder der Linux- bzw. Windows-Maschine durch die gesicherte Datei.
- Häufigkeit der Sicherungsvorgänge – Stellen Sie sicher, dass die Häufigkeit der Sicherungsvorgänge und die Sicherungstypen basierend auf den verfügbaren Ressourcen und den kundenspezifischen Anforderungen entsprechend ausgewählt werden.
- Zeitplan der Sicherungsvorgänge – Berücksichtigen Sie die folgenden Richtlinien beim Planen von regelmäßigen Sicherungen.
  - Bei den meisten Tools, mit deren Hilfe Sicherungs- oder Replizierungsvorgänge durchgeführt werden, kann es bei einem angemessen ausgelasteten Cluster-Setup beim erstmaligen Auslösen der Datensicherung eine Weile dauern, bis der erste Sicherungsvorgang abgeschlossen ist – egal, welches Tool verwendet wurde.
  - Allerdings handelt es sich in der Regel bei der erstmaligen Sicherung um eine vollständige Datensicherung. Die nächsten Sicherungsvorgänge, bei denen es sich um inkrementelle oder vollständige Datensicherungen handeln kann, werden im Vergleich zum erstmaligen Sicherungsvorgang schneller durchgeführt.

- Replizierungstyp – Die Wahl des Replizierungstyps ist auch bei der Konfiguration einer virtuellen Maschine für die Notfallwiederherstellung entscheidend. Berücksichtigen Sie bei Ihrer Entscheidung für einen Replizierungstyp die Zielvorgaben für den Wiederanlaufpunkt (RPO) und die Wiederanlaufzeit (RTO) sowie die Kosten und die Skalierbarkeit.
- Gleichzeitig durchgeführte Sicherungsaufgaben – Wenn Ressourcen kein Thema sind und das gleichzeitige Sichern von Clusterknoten vom Tool unterstützt wird, wird empfohlen, dies zu aktivieren, um den Sicherungsvorgang zu beschleunigen. Sichern Sie alle Knoten gleichzeitig.
- Überwachen – Während der Sicherungsvorgang läuft, achten Sie auf etwaige Umgebungs- und Leistungsprobleme in der vRealize Log Insight-Konfiguration. Die meisten Datensicherungs-, Wiederherstellungs- und Notfallwiederherstellungs-Tools stellen Überwachungsfunktionen zur Verfügung.
  - Überprüfen Sie während des Sicherungsvorgangs alle relevanten Protokolle auf dem Produktionssystem, da möglicherweise nicht alle Probleme auf der Benutzeroberfläche angezeigt werden.

Richtlinien für die Wiederherstellung und die Notfallwiederherstellung

Bestimmte Richtlinien für die Wiederherstellung und die Notfallwiederherstellung bieten zusätzliche Best Practices.

- Wiederherstellungsstatus – Achten Sie darauf, dass sich die wiederhergestellten Knoten im Zustand „Ausgeschaltet“ befinden. Es wird empfohlen, wie nachfolgend beschrieben die Knoten in einer bestimmten Reihenfolge wiederherzustellen und manuelle Konfigurationsänderungen in einigen Wiederherstellungsszenarios anzuwenden.
- Wiederherstellungsreihenfolge – Stellen Sie sicher, dass der vRealize Log Insight-Masterknoten vor den Worker-Knoten wiederhergestellt wird. Die Worker-Knoten können in beliebiger Reihenfolge wiederhergestellt werden. Sobald der vRealize Log Insight-Server (bei einer Clusterkonfiguration der Masterknoten und alle Worker-Knoten) wiederhergestellt wurde, stellen Sie die Weiterleitungsinstanzen wieder her, sofern sie konfiguriert sind, ggf. gefolgt von den wiederhergestellten Agenten.
- Wiederherstellungsziel – Je nach Wiederherstellungs-Tool können die virtuellen Maschinen auf demselben Host, auf einem anderen Host in demselben Datencenter oder auf einem anderen Host in einem Remote-Ziel-Datencenter wiederhergestellt werden.
  - Bei einem Notfallwiederherstellungszenario können Sie manchmal nicht auf derselben Site wiederherstellen, weil die primäre Site vollständig ausgefallen ist, aber je nach ausgewählter Option gibt es einige manuelle Schritte, die erforderlich sind, um den vRealize Log Insight-Cluster vollständig wiederherzustellen und ihn in einen ausführbaren Zustand zu versetzen.
  - Wenn der vRealize Log Insight-Cluster nicht vollständig ausgefallen ist und darauf zugegriffen werden kann, stellen Sie sicher, dass die Clusterinstanzen ausgeschaltet sind, bevor Sie den Cluster auf einer neuen Site wiederherstellen.
  - Achten Sie darauf, dass es kein Split-Brain-Verhalten gibt, wenn dieselben IP-Adressen und/oder FQDNs auf der Wiederherstellungs-Site verwendet werden. Stellen Sie sicher, dass niemand versehentlich einen teilweise funktionierenden Cluster auf der primären Site verwendet.
- IP-Anpassung – Wenn dieselben IP-Adressen beim Wiederherstellen eines vRealize Log Insight-Clusters verwendet werden, achten Sie darauf, dass die IP-Adressen und FQDNs aller wiederhergestellten Knoten den entsprechenden ursprünglichen Gegenstücken zugeordnet sind. Das folgende Szenario beispielsweise schlägt fehl: Ein Cluster hat drei Knoten, A, B und C. Knoten A wird mit der IP-Adresse von B, und/oder Knoten B wird mit der IP-Adresse von C und/oder Knoten C wird mit der IP-Adresse von A wiederhergestellt.
  - Wenn dieselben IP-Adressen nur für einen Teil der wiederhergestellten Knoten verwendet werden, sollten Sie für diese Knoten sicherstellen, dass allen wiederhergestellten Images deren ursprüngliche IP-Adresse zugeordnet wird.

- Wiederherstellungsplan – Bei einem Ausfall oder Notfall wird empfohlen, so bald wie möglich den vRealize Log Insight-Cluster wiederherzustellen. Das Vorhandensein eines gut dokumentierten und getesteten Wiederherstellungsplans ist sehr wichtig, um den Cluster wieder funktionsfähig zu machen.
- Überwachung – Die meisten Sicherungs-, Wiederherstellungs- und Notfallwiederherstellungs-Tools bieten eine Art Überwachungsansicht, damit Sie den Fortschritt der Wiederherstellungsvorgänge live verfolgen können und somit Fehlschläge oder Warnungen nicht übersehen. Achten Sie darauf, dass Sie geeignete Maßnahmen zum Beheben von Problemen ergreifen.
- Konfigurationsänderungen nach der Wiederherstellung – Falls manuelle Konfigurationsänderungen erforderlich sind, bevor die Site vollständig wiederhergestellt werden kann, halten Sie sich an die Richtlinien unter „Richtlinien für Konfigurationsänderungen nach der Wiederherstellung“, auf Seite 96.
- Validierung – Führen Sie nach einer erfolgreichen Wiederherstellung eine kurze Prüfung des wiederhergestellten Clusters durch.

Richtlinien für Konfigurationsänderungen nach der Wiederherstellung

Je nach Wiederherstellungsziel und die während der Sicherungskonfiguration angewendeten IP-Anpassungen sind manuelle Konfigurationsänderungen für einen oder mehrere vRealize Log Insight-Knoten erforderlich, bevor die wiederhergestellte Site voll funktionsfähig werden kann.

Wiederherstellen auf demselben Host

Der Vorgang für das Wiederherstellen eines vRealize Log Insight-Clusters auf demselben Host sollte unkompliziert sein und kann mit jedem Tool durchgeführt werden,.

- Wenn möglich, sollten alle für die Produktionsumgebung verwendeten Netzwerk-, IP- und FQDN-Einstellungen auf der wiederhergestellten Site aufbewahrt werden.
- Während des Wiederherstellungsvorgangs wird die ursprüngliche Kopie des Clusters durch die wiederhergestellte Version überschrieben, es sei denn, es wird ein neuer Name für die virtuelle Maschine angegeben.
- Wenn, wie in den Standardeinstellungen angegeben, dieselben IP-Adressen und FQDNs für die wiederhergestellten Clusterknoten verwendet werden, schalten Sie den vorhandenen Cluster aus, bevor Sie mit dem Wiederherstellungsvorgang beginnen.
- Löschen Sie nach einer erfolgreichen Wiederherstellung und einer erfolgreichen Plausibilitätsprüfung die alte Kopie, um Ressourcen zu schonen und mögliche versehentliche Split-Brain-Situationen zu verhindern, bei denen ein Benutzer die alte Kopie einschalten könnte.

Wiederherstellen auf einem anderen Host

Für das Wiederherstellen auf einem anderen Host sind manuelle Konfigurationsänderungen auf dem vRealize Log Insight-Cluster erforderlich. Siehe „Wiederherstellen auf einem anderen Host“, auf Seite 97 für weitere Informationen zu den spezifischen Änderungen für vRealize Log Insight 3.0 GA- und 2.5 GA-Builds, die für jedes Sicherungs- und Wiederherstellungs-Tool verwendet werden können. Es wird vorausgesetzt, dass den wiederhergestellten vRealize Log Insight-Knoten andere IP-Adressen und FQDNs als den entsprechenden Quellknoten zugewiesen wurden, die gesichert wurden.

Wiederherstellen von vRealize Log Insight -Ereignisweiterleitungen

Die Anweisungen für das manuelle Wiederherstellen von vRealize Log Insight-Ereignisweiterleitungen entsprechen den oben beschriebenen Anweisungen für vRealize Log Insight Server.

Wiederherstellen von vRealize Log Insight -Agenten

Wenn das gesamte Agentenbetriebssystem gesichert wurde, halten Sie sich an den spezifischen Workflow für das Tool, um das Agentenbetriebssystem wiederherzustellen.

- Wenn die Agentenkonfiguration clientseitig (auf dem Agentenbetriebssystem) vorgenommen wurde, ersetzen Sie die Datei „agent.ini“ durch die Sicherungskopie.
- Wenn Konfigurationsänderungen nur serverseitig (auf dem vRealize Log Insight-Masterknoten) vorgenommen werden, müssen die virtuellen Agenten-Maschinen nicht gesichert und wiederhergestellt werden.

Validieren der Wiederherstellung

Sie müssen sicherstellen, dass alle wiederhergestellten vRealize Log Insight-Cluster voll funktionsfähig sind.

- Stellen Sie sicher, dass Sie mithilfe der IP-Adresse oder des FQDN (sofern konfiguriert) des internen Lastausgleichsdiensts auf die Benutzeroberfläche von vRealize Log Insight sowie unter Verwendung der jeweiligen IP-Adressen oder FQDNs auf alle individuellen Clusterknoten zugreifen können.
- Von der Seite vRealize Log Insight Verwaltung aus:
  - Verifizieren Sie den Status der Clusterknoten von der Clusterseite aus und stellen Sie sicher, dass sich der interne Lastausgleichsdienst (sofern konfiguriert) im Zustand „Aktiv“ befindet.
  - Prüfen Sie die vSphere-Integration. Falls erforderlich, konfigurieren Sie die Integration neu. Dies geschieht, wenn nach der Wiederherstellung die IP-Adresse bzw. der FQDN des Masterknotens und/oder des internen Lastausgleichsdiensts geändert wird.
  - Prüfen Sie die vRealize Operations Manager-Integration und konfigurieren Sie sie bei Bedarf neu.
  - Stellen Sie sicher, dass alle Inhaltspakete und Funktionen der Benutzeroberfläche ordnungsgemäß funktionieren.
  - Verifizieren Sie auch, dass die vRealize Log Insight-Ereignisweiterleitungen und -Agenten ordnungsgemäß funktionieren, sofern diese konfiguriert sind.
- Stellen Sie sicher, dass die anderen wichtigen Funktionen von vRealize Log Insight wie erwartet funktionieren.

Wiederherstellen auf einem anderen Host

Wenn Sie auf einen anderen Host wiederherstellen, müssen Sie auf dem vRealize Log Insight-Cluster Konfigurationsänderungen vornehmen.

Diese Aufgabe beschreibt die Konfigurationsänderungen für die vRealize Log Insight-Builds 3.0 GA und 2.5 GA, die für jedes Backup-Wiederherstellungs-Tool verwendet werden können. Es wird vorausgesetzt, dass den wiederhergestellten vRealize Log Insight-Knoten andere IP-Adressen und FQDNs als den entsprechenden Quellknoten zugewiesen wurden, die gesichert wurden.

Voraussetzungen

Lesen Sie die Richtlinien und Empfehlungen in Kapitel 8, „Sichern, Wiederherstellen und die Notfallwiederherstellung“, auf Seite 91 durch.

Vorgehensweise

1 Listen Sie alle neuen IP-Adressen und FQDNs auf, die jedem vRealize Log Insight-Knoten zugewiesen wurden.

2 Nehmen Sie die folgenden Konfigurationsänderungen auf dem Masterknoten vor:

a Schalten Sie den Masterknoten ein, falls er nicht bereits eingeschaltet ist.

HINWEIS Die Schritte b bis e gelten für den vRealize Log Insight-Build 2.5 GA. Ab vRealize Log Insight 3.0 GA wird das direkte Ändern der Konfigurationsdateien von der Appliance-Konsole aus nicht offiziell unterstützt. In diesem KnowledgeBase-Artikel finden Sie weitere Informationen über das Vornehmen dieser Änderungen mithilfe der Web-UI-Benutzeroberfläche in vRealize Log Insight 3.0 GA.

---

b Verwenden Sie SSH, um die Verbindung zur virtuellen Appliance des Knotens als Root-Benutzer herzustellen.

c Falls der vRealize Log Insight-Dienst ausgeführt wird, halten Sie den Dienst mit dem folgenden Befehl an: `service loginsight stop`.

d Führen Sie `cd /storage/core/loginsight/config` aus.

e Führen Sie `cp loginsight-config.xml#<n> backup-loginsight-config.xml` aus, wobei `<n>` die höchste Nummer ist, die automatisch während Konfigurationsänderungen an `loginsight-config.xml` angehängt wird.

f Öffnen Sie die kopierte Version der Konfigurationsdatei in einem Texteditor (oder wie oben empfohlen in der vRealize Log Insight 3.0 GA-Web-Benutzeroberfläche) und suchen Sie nach Zeilen ähnlich den folgenden. Diese Konfigurationsänderung gilt für vRealize Log Insight 3.0 GA und 2.5 GA.

```
<distributed overwrite-children="true">
  <daemon host="prod-es-vrli1.domain.com" port="16520" token="c4c4c6a7-f85c-4f28-
a48f-43aeea27cd0e">
    <service-group name="standalone" />
  </daemon>
  <daemon host="192.168.1.73" port="16520" token="a5c65b52-aff5-43ea-8a6d-38807ebc6167">
    <service-group name="workernode" />
  </daemon>
  <daemon host="192.168.1.74" port="16520" token="a2b57cb5-a6ac-48ee-8e10-17134e1e462e">
    <service-group name="workernode" />
  </daemon>
</distributed>
```

g Im obigen Codeausschnitt gibt es drei Knoten: Der erste Knoten ist der Masterknoten, bei dem `<service-group name=standalone>` steht, und die anderen zwei Knoten sind Worker-Knoten, bei denen `<service-group name="workernode">` steht.

h Prüfen Sie in der neu wiederhergestellten Umgebung für den Masterknoten, ob der in der Umgebung vor der Wiederherstellung verwendete DNS-Eintrag wiederverwendet werden kann.

- Falls der DNS-Eintrag wiederverwendet werden kann, müssen Sie den DNS-Eintrag lediglich so ändern, dass er auf die neue IP-Adresse des Masterknotens verweist.
- Kann der DNS-Eintrag nicht wiederverwendet werden, ersetzen Sie den Eintrag für den Masterknoten durch den neuen DNS-Namen (der auf die neue IP-Adresse verweist).
- Falls der DNS-Name nicht zugewiesen werden kann, aktualisieren Sie als letzte Option den Konfigurationseintrag mit der neuen IP-Adresse.

i Aktualisieren Sie zudem die IP-Adressen der Worker-Knoten entsprechend den neuen IP-Adressen.

j Durchsuchen Sie dieselbe Konfigurationsdatei nach Einträgen, die NTP-, SMTP- sowie Datenbank- und „appender“-Abschnitte darstellen.

Dies gilt für vRealize Log Insight 3.0 GA und 2.5 GA.

HINWEIS Der Abschnitt `<logging><appenders>...</appenders></logging>` gilt nur für den Build vRealize Log Insight 2.5 GA und ist in vRealize Log Insight 3.0 GA nicht verfügbar.

```
<ntp>
  <ntp-servers value="ntp1.domain.com, ntp2.domain.com" />
</ntp>

<smtp>
  <server value="smtp.domain.com" />
  <default-sender value="source.domain.com@domain.com" />
</smtp>

<database>
  <password value="xserttt" />
  <host value="vrli-node1.domain.com" />
  <port value="12543" />
</database>

<logging>
  <appenders>
    <appender name="REMOTE" class="com.vmware.loginsight.commons.logging.ThriftSocketAp-
pender">
      <param name="RemoteHost" value="vdli-node1.domain.com" />
    </appender>
  </appenders>
</logging>
```

- Wenn in der neuen Umgebung die konfigurierten Werte des NTP-Servers nicht mehr gültig sind, passen Sie diese im Abschnitt `<ntp>...</ntp>` an.
- Wenn in der neuen Umgebung die konfigurierten Werte des SMTP-Servers nicht mehr gültig sind, passen Sie diese im Abschnitt `<smtp>...</smtp>` an.
- Optional können Sie auch den Wert für `default-sender` im SMTP-Abschnitt ändern. Es kann sich dabei um einen beliebigen Wert handeln, es wird jedoch empfohlen, einen Wert anzugeben, der die Quelle angibt, von wo aus die E-Mail gesendet wird.
- Ändern Sie im Abschnitt `<database>..</database>` den Wert für den Host, so dass er auf den FQDN oder die IP-Adresse des Masterknotens verweist.
- Ändern Sie im Abschnitt `<logging><appenders>...</appenders></logging>` den Parameterwert für `RemoteHost` entsprechend dem neuen FQDN bzw. der neuen IP-Adresse des Masterknotens.

k Aktualisieren Sie in derselben Konfigurationsdatei den vRealize Log Insight ILB-Konfigurationsabschnitt

Bei einer vRealize Log Insight 3,0 GA-Appliance:

```
<load-balancer>
<leadership-lease-renewal-secs value="5" />
<high-availability-enabled value="true" />
<high-availability-ip value="10.158.128.165" />
<high-availability-fqdn value="LB-FQDN.eng.vmware.com" />
<layer4-enabled value="true" />
<ui-balancing-enabled value="true" />
</load-balancer>
```

Bei einer vRealize Log Insight 2.5 GA-Appliance:

```
<load-balancer>
  <leadership-lease-renewal-secs value="5" />
  <high-availability-enabled value="true" />
  <high-availability-ip value="192.168.1.75" />
  <layer4-enabled value="true" />
</load-balancer>
```

l Ändern Sie im Abschnitt `<load-balancer>...</load-balancer>` den Wert von `high-availability-ip`, falls er sich von der aktuellen Einstellung unterscheidet.

m Achten Sie bei vRealize Log Insight 3.0 GA darauf, dass Sie auch den FQDN des Lastausgleichsdiensts anpassen.

n Benennen Sie die aktualisierte Konfigurationsdatei um, um die Änderungen abzuschließen.

HINWEIS Dieser Schritt gilt nur für vRealize Log Insight 2.5 GA. In vRealize Log Insight 3.0 GA werden die Änderungen über die Web-Benutzeroberfläche vorgenommen.

Führen Sie `: mv backup-loginsight-config.xml loginsight-config.xml#<n+1>` aus, wobei `n` die aktuell höchste Nummer ist, die an die `loginsight-config.xml`-Dateien angehängt wird.

o Für vRealize Log Insight 2.5 GA starten Sie den vRealize Log Insight-Dienst neu; führen Sie dazu folgenden Befehl aus: `service loginsight start`.

HINWEIS Dies kann in vRealize Log Insight 3.0 GA über die Web-Benutzeroberfläche vorgenommen werden, indem Sie zur Registerkarte „Cluster“ auf der Seite „Verwaltung“ gehen. Wählen Sie für jeden aufgeführten Knoten dessen Hostnamen oder IP-Adresse aus, um den Detailbereich zu öffnen, und klicken Sie auf Log Insight neu starten. Die Konfigurationsänderungen werden automatisch auf alle Clusterknoten angewendet.

p Warten Sie zwei Minuten nach dem Start des vRealize Log Insight-Diensts, um genügend Zeit zu lassen, bis die Cassandra-Dienste aktiv werden, bevor Sie die anderen Worker-Knoten online bringen.

HINWEIS Überspringen Sie die Schritte 3 bis 9 bei vRealize Log Insight 3.0 GA. Diese Schritte gelten nur für vRealize Log Insight 2.5 GA. Folgen Sie bei vRealize Log Insight 3.0 GA den Anweisungen in Schritt 2. (o) dieses Themas, um die Konfigurationsänderungen auf alle Worker-Knoten anzuwenden.

3 Führen Sie SSH auf den ersten Worker-Knoten unter Verwendung der Root-Anmeldedaten aus.

4 Halten Sie den vRealize Log Insight-Dienst an und führen Sie `: service loginsight stop` aus.

5 Kopieren Sie die neueste `loginsight-conig.xml`-Datei vom Masterknoten auf den Worker-Knoten.

6 Führen Sie auf dem Worker-Knoten `: scp root@[master-node-ip]:/storage/core/loginsight/config/loginsight-config.xml#<n> /storage/core/loginsight/config/` aus

7 Führen Sie `: service loginsight start` aus.

8 Warten Sie zwei Minuten nach dem Start des vRealize Log Insight-Diensts, um genügend Zeit für den Start des Cassandra-Diensts zu lassen.

9 Wiederholen Sie die Schritte 3 bis 6 für jeden Worker-Knoten.

Fehlerbehebung bei vRealize Log Insight 9

Bevor Sie sich an die VMware Support-Dienste wenden, können Sie allgemeine Probleme, die mit der Verwaltung von vRealize Log Insight in Zusammenhang stehen, selbst beheben.

Dieses Kapitel behandelt die folgenden Themen:

- „Es gehen keine ESXi-Protokolle mehr in vRealize Log Insight ein“, auf Seite 103
- „vRealize Log Insight steht zu wenig Festplattenspeicher zur Verfügung“, auf Seite 104
- „Herunterladen eines Support-Pakets für vRealize Log Insight“, auf Seite 105
- „Erstellen eines Support-Pakets von vRealize Log Insight über die Virtual Appliance-Konsole“, auf Seite 105
- „Zurücksetzen des Admin-Benutzerkennworts“, auf Seite 106
- „Zurücksetzen des Root-Benutzerkennworts“, auf Seite 106
- „Warnungen konnten nicht an vRealize Operations Manager gesendet werden“, auf Seite 107
- „Anmeldung unter Verwendung der Active Directory-Anmeldedaten nicht möglich“, auf Seite 108
- „SMTP funktioniert bei aktivierter STARTTLS-Option nicht“, auf Seite 108
- „Fehlschlagen des Upgrades, weil die Signatur der PAK-Datei nicht validiert werden kann“, auf Seite 109
- „Fehlschlagen des Upgrades mit einem internen Serverfehler“, auf Seite 110

Es gehen keine ESXi -Protokolle mehr in vRealize Log Insight ein

Nach einem Neustart des vRealize Log Insight-Dienstes gehen keine Syslog-Meldungen von ESXi-Hosts mehr in vRealize Log Insight ein.

Problem

Aufgrund von Konfigurationsänderungen in vRealize Log Insight ist ein Neustart des vRealize Log Insight-Dienstes erforderlich. Nach dem Neustart sind keine Syslog-Feeds von ESXi mehr verfügbar.

Ursache

Bestimmte ESXi-Versionen senden keine Protokolle mehr, wenn die Verbindung zum Remote-Syslog-Listener auch nur kurzzeitig unterbrochen wird. Dieses Problem betrifft je nach verwendetem Kommunikationsprotokoll die folgenden ESXi-Versionen:

Tabelle 9-1. ESXi-Versionen, die das Versenden von Syslog-Meldungen einstellen

Kommunikationsprotokoll	Betroffene ESXi-Version
TCP	■ ESXi 5.0.x ■ ESXi 5.1.x
UDP	ESXi 5.0 und 5.0 Update 1

Wichtig Dieses Problem wurde in ESXi 5.1 Update 2 und ESXi 5.0, Patch ESXi500-201401401-BG, behoben. VMware empfiehlt Ihnen, das Update oder den Patch anzuwenden, um sicherzustellen, dass Ihre ESXi-Hosts das Versenden von Syslog-Meldungen an ihre Remote-Ziele nicht unterbrechen. Weitere Informationen finden Sie unter https://www.vmware.com/support/vsphere5/doc/vsphere-esxi-51u2-release-notes.html und VMware ESXi 5.0, Patch ESXi500-201401401-BG: Updates esx-base (2065691). Wenn Sie das Update oder Patch nicht anwenden möchten, verwenden Sie die folgende Lösung.

Lösung

1 Klicken Sie auf das Dropdown-Menüsymbol für die Konfiguration und wählen Sie **Verwaltung** aus.

2 Klicken Sie unter „Integration“ auf **vSphere**.

3 Klicken Sie bei jeder vCenter Server-Instanz, bei der der Link **ESXi-Syslog-Konfigurationsinformationen anzeigen** vorhanden ist, auf den Link **ESXi-Syslog-Konfigurationsinformationen anzeigen**.

4 Wählen Sie alle Hosts aus, die zuvor konfiguriert waren und klicken Sie auf **Konfigurieren**.

Hinweis Der Konfigurationsvorgang kann einige Minuten dauern. Sie müssen diesen Vorgang bei jedem Neustart von vRealize Log Insight wiederholen. Weitere Informationen zu Syslog-Problemen und -Lösungen, siehe VMware ESXi 5.x-Host sendet keine Syslogs mehr an den Remote-Server (2003127).

vRealize Log Insight steht zu wenig Festplattenspeicher zur Verfügung

Die Speicherkapazität eines vRealize Log Insight-Master- oder Worker-Knotens kann möglicherweise überschritten werden, wenn Sie eine kleine virtuelle Festplatte verwenden und keine Archivierung aktiviert ist.

Problem

vRealize Log Insight steht zu wenig Festplattenspeicher zur Verfügung, wenn der Anteil der eingehenden Protokolle 3 Prozent des Speicherplatzes pro Minute überschreitet.

Ursache

Im Normalfall wird die Speicherkapazität von vRealize Log Insight nie überschritten, da jede Minute geprüft wird, ob der freie Speicherplatz weniger als 3 Prozent beträgt. Wenn der freie Speicherplatz auf der virtuellen vRealize Log Insight-Appliance unter 3 Prozent fällt, werden alte Daten-Buckets stillgelegt.

Ist die Festplatte jedoch klein und die Protokollaufnahmerate so hoch, dass der freie Speicherplatz (3 Prozent) innerhalb von 1 Minute vollständig in Anspruch genommen wird, wird die Speicherkapazität von vRealize Log Insight überschritten.

Bei aktivierter Archivierung archiviert vRealize Log Insight das Bucket vor dessen Stilllegung. Wenn der freie Speicherplatz voll belegt ist, bevor das alte Bucket archiviert und stillgelegt wurde, steht vRealize Log Insight zu wenig Festplattenspeicher zur Verfügung.

Lösung

◆ Erhöhen Sie die Speicherkapazität der virtuellen vRealize Log Insight-Appliance. Weitere Informationen hierzu finden Sie unter „Erhöhen der Speicherkapazität der virtuellen vRealize Log Insight-Appliance“, auf Seite 18.

Herunterladen eines Support-Pakets für vRealize Log Insight

Falls vRealize Log Insight aufgrund eines Problems nicht wie erwartet funktioniert, können Sie eine Kopie der Protokoll- und Konfigurationsdateien an die VMware Support-Dienste senden.

Voraussetzungen

Vergewissern Sie sich, dass Sie bei der Web-Benutzeroberfläche von vRealize Log Insightals Benutzer mit der Berechtigung **Admin bearbeiten** angemeldet sind. Das URL-Format lautet https://*log-insight-host*, wobei *log-insight-host* die IP-Adresse oder der Hostname der virtuellen vRealize Log Insight-Appliance ist.

Vorgehensweise

1 Klicken Sie auf das Dropdown-Menüsymbol für die Konfiguration und wählen Sie **Verwaltung** aus.

2 Klicken Sie unter „Verwaltung“ auf **Appliance**.

3 Klicken Sie unter dem Support-Header auf **Support-Paket herunterladen**.

Das vRealize Log Insight-System erfasst die Diagnoseinformationen und streamt die Daten in einem komprimierten Tarball an Ihren Browser.

4 Klicken Sie im Dialogfeld „Datei-Download“ auf **Speichern**.

5 Wählen Sie das Verzeichnis aus, in dem Sie das Tarball-Archiv speichern möchten, und klicken Sie auf **Speichern**.

Weiter

Sie können den Inhalt der Protokolldateien auf Fehlermeldungen überprüfen. Wenn Sie Probleme behoben haben, löschen Sie das veraltete Support-Paket, um Festplattenspeicher freizugeben.

Erstellen eines Support-Pakets von vRealize Log Insight über die Virtual Appliance-Konsole

Wenn Sie nicht auf die Web-Benutzeroberfläche von vRealize Log Insight zugreifen können, können Sie mithilfe der Konsole der virtuellen Appliance oder nach Herstellung einer SSH-Verbindung zur virtuellen Appliance von vRealize Log Insight das Support-Paket herunterladen.

Voraussetzungen

- Stellen Sie sicher, dass Sie über die Root-Benutzer-Anmeldedaten verfügen, um sich bei der virtuellen vRealize Log Insight-Appliance anzumelden.
- Wenn Sie eine Verbindung zu einer virtuellen vRealize Log Insight-Appliance unter Verwendung von SSH herstellen möchten, stellen Sie sicher, dass TCP-Port 22 geöffnet ist.

Vorgehensweise

1 Stellen Sie eine SSH-Verbindung zur vRealize Log Insight-vApp her und melden Sie sich als Root-Benutzer an.

2 Führen Sie zur Erstellung des Support-Pakets `loginsight-support` aus.

Die Support-Informationen werden erfasst und in einer `*.tar.gz`-Datei mit der folgenden Benennungskonvention gespeichert: `loginsight-support-YYYY-MM-DD_HHMMSS.xxxxx.tar.gz`, wobei `xxxxx` für die Prozess-ID steht, unter der der Prozess `loginsight-support`ausgeführt wurde.

Weiter

Leiten Sie das Support-Paket wie verlangt an die VMware Support-Dienste weiter.

Zurücksetzen des Admin-Benutzerkennworts

Wenn ein Admin-Benutzer das Kennwort für die Web-Benutzeroberfläche vergisst, ist das Konto nicht mehr erreichbar.

Problem

Wenn es nur einen Admin-Benutzer für vRealize Log Insight gibt und der Admin-Benutzer das Kennwort vergisst, kann die Anwendung nicht verwaltet werden. Wenn ein Admin-Benutzer der einzige Benutzer von vRealize Log Insight ist, kann auf die gesamte Web-Benutzeroberfläche nicht mehr zugegriffen werden.

Ursache

In vRealize Log Insight gibt es keine Benutzeroberfläche, in der Admin-Benutzer ihre eigenen Kennwörter zurücksetzen können, wenn ein Benutzer sich nicht an das aktuelle Kennwort erinnert.

Hinweis Admin-Benutzer, die sich anmelden können, können das Kennwort anderer Admin-Benutzer zurücksetzen. Setzen Sie das Admin-Benutzerkennwort nur zurück, wenn von allen Admin-Benutzerkonten kein Kennwort bekannt ist.

Lösung

Voraussetzungen

- Stellen Sie sicher, dass Sie über die Root-Benutzer-Anmeldedaten verfügen, um sich bei der virtuellen vRealize Log Insight-Appliance anzumelden. Siehe „Konfigurieren des SSH-Root-Kennworts für die virtuelle Log Insight-Appliance“, auf Seite 16.
- Um SSH-Verbindungen zu aktivieren, überprüfen Sie zunächst, ob der TCP-Port 22 geöffnet ist.

Vorgehensweise

1. Stellen Sie eine SSH-Verbindung zur virtuellen vRealize Log Insight-Appliance her und melden Sie sich als Root-Benutzer an.
2. Geben Sie `li-reset-admin-passwd.sh` ein und drücken Sie die **Eingabetaste**.

   Das Skript setzt das Admin-Benutzerkennwort zurück, erstellt ein neues Kennwort und zeigt dieses auf dem Bildschirm an.

Weiter

Melden Sie sich mit dem neuen Kennwort bei der Web-Benutzeroberfläche von vRealize Log Insight an und ändern Sie das Admin-Benutzerkennwort.

Zurücksetzen des Root-Benutzerkennworts

Wenn Sie das Kennwort des Root-Benutzers vergessen, können Sie keine SSH-Verbindungen mehr herstellen oder die Konsole der virtuellen vRealize Log Insight-Appliance verwenden.

Problem

Wenn Sie keine SSH-Verbindungen herstellen oder die Konsole der virtuellen vRealize Log Insight-Appliance nicht verwenden können, können Sie bestimmte Verwaltungsaufgaben nicht ausführen und das Kennwort des Admin-Benutzers nicht zurücksetzen.

Lösung

1. Starten Sie in vSphere Client das Gastbetriebssystem der virtuellen vRealize Log Insight-Appliance und öffnen Sie die Konsole für die virtuelle Maschine.

2 Klicken Sie auf die Konsole, warten Sie, bis das GRUB-Menü angezeigt wird, und drücken Sie eine beliebige Buchstabentaste.

HINWEIS Die GRUB-Eingabeaufforderung wird 7 Sekunden lang auf dem Bildschirm angezeigt, bevor sie die Startsequenz anstößt.

3 Wählen Sie im GRUB-Menü mit den Pfeiltasten **SUSE Linux Enterprise Server für VMware**.

4 Drücken Sie die Leertaste, geben Sie **`init=/bin/sh`** ein und drücken Sie die Eingabetaste.

Der Kernel startet im Shell-Modus.

5 Geben Sie in der Shell **`passwd`** ein, drücken Sie die Eingabetaste und folgen Sie den Anweisungen auf dem Bildschirm, um das Root-Kennwort zu ändern.

Das Kennwort muss aus mindestens acht Zeichen bestehen und mindestens einen Großbuchstaben, einen Kleinbuchstaben, eine Ziffer und ein Sonderzeichen wie $ oder & enthalten. Sie können dasselbe Zeichen nicht mehr als vier Mal wiederholen.

6 Geben Sie in der Shell **`reboot`** ein.

Weiter

Prüfen Sie, sobald Log Insight neu gestartet wird, ob Sie sich als Root-Benutzer anmelden können.

Warnungen konnten nicht an vRealize Operations Manager gesendet werden

vRealize Log Insight benachrichtigt Sie, wenn ein Warnungsereignis nicht an vRealize Operations Manager gesendet werden kann. vRealize Log Insight wiederholt das Senden der Warnung jede Minute, bis das Problem behoben ist.

Problem

In der Symbolleiste von vRealize Log Insight wird ein rotes Symbol mit einem Ausrufezeichen angezeigt, wenn eine Warnung nicht an vRealize Operations Manager übermittelt werden konnte.

Ursache

Aufgrund von Verbindungsproblemen kann vRealize Operations Manager vRealize Log Insight keine Warnungsbenachrichtigungen an vRealize Operations Manager versenden.

Lösung

- Klicken Sie auf das rote Symbol, um die Liste der Fehlermeldungen zu öffnen, und scrollen Sie nach unten, um die aktuellste Nachricht anzuzeigen.

  Das rote Zeichen verschwindet von der Symbolleiste, wenn Sie die Liste der Fehlermeldungen öffnen oder das Problem behoben ist.

- Versuchen Sie, mit den folgenden Anweisungen das Verbindungsproblem mit vRealize Operations Manager zu beheben:
  - Stellen Sie sicher, dass die vRealize Operations Manager-vApp nicht heruntergefahren wurde.
  - Überprüfen Sie, ob Sie sich mit vRealize Operations Manager über die Schaltfläche **Verbindung testen** im Abschnitt **vRealize Operations Manager** der Seite **Verwaltung** der vRealize Log Insight-Web-Benutzeroberfläche verbinden können.
  - Stellen Sie sicher, dass Sie über die richtigen Anmeldedaten verfügen, indem Sie sich direkt bei vRealize Operations Manager anmelden.
  - Überprüfen Sie die Protokolle aus vRealize Log Insight und vRealize Operations Manager auf Meldungen, die auf Verbindungsprobleme hinweisen.

- Vergewissern Sie sich, dass keine Warnungen in der vRealize Operations Manager vSphere-Benutzeroberfläche herausgefiltert werden.

Anmeldung unter Verwendung der Active Directory-Anmeldedaten nicht möglich

Sie können sich nicht bei der Web-Benutzeroberfläche von vRealize Log Insight anmelden, wenn Sie Active Directory-Anmeldedaten verwenden.

Problem

Sie können sich nicht mit Ihren Anmeldedaten für die Active Directory-Domäne bei vRealize Log Insight anmelden, obwohl ein Administrator Ihr Active Directory-Konto in vRealize Log Insight aufgenommen hat.

Ursache

Die häufigsten Ursachen hierfür sind abgelaufene Kennwörter, falsche Anmeldedaten, Verbindungsprobleme oder mangelnde Uhrzeitsynchronisation zwischen der virtuellen vRealize Log Insight-Appliance und Active Directory.

Lösung

- Vergewissern Sie sich, dass Ihre Anmeldedaten gültig sind, Ihr Kennwort nicht abgelaufen und Ihr Active Directory-Konto nicht gesperrt ist.
- Wenn Sie keine Domäne zur Verwendung mit Active-Directory-Authentifizierung angegeben haben, stellen Sie sicher, dass Sie ein Konto auf der Standarddomäne haben, die in der neuesten vRealize Log Insight-Konfiguration unter `/storage/core/loginsight/config/loginsight-config.xml#[number]` gespeichert ist, wobei [Ziffer] die höchste Ziffer ist.
- Suchen Sie die neueste Konfigurationsdatei: `/storage/core/loginsight/config/loginsight-config.xml#[number]`, wobei `[number]` die höchste Ziffer ist.
- Stellen Sie sicher, dass vRealize Log Insight über eine Verbindung zum Active Directory-Server verfügt.
  - Begeben Sie sich zum **Authentifizierungsabschnitt** der **Verwaltungsseite** der vRealize Log Insight Web-Benutzeroberfläche, geben Sie Ihre Anmeldedaten ein und klicken Sie auf die Schaltfläche **Verbindung testen**.
  - Überprüfen Sie, ob in vRealize Log Insight `/storage/var/loginsight/runtime.log` mit DNS-Problemen verbundene Meldungen vorhanden sind.
- Stellen Sie sicher, dass die Uhrzeiten in vRealize Log Insight und Active Directory zueinander synchron sind.
  - Überprüfen Sie, ob in vRealize Log Insight `/storage/var/loginsight/runtime.log` mit Taktverschiebungen verbundene Meldungen vorhanden sind.
  - Verwenden Sie einen NTP-Server, um die Uhrzeiten von vRealize Log Insight und Active Directory zu synchronisieren.

SMTP funktioniert bei aktivierter STARTTLS-Option nicht

Bei der Konfiguration des SMTP-Servers mit aktivierter STARTTLS-Option schlägt der Versand von Test-E-Mails fehl. Fügen Sie Ihr SSL-Zertifikat für den SMTP-Server dem Java-Truststore hinzu, um das Problem zu beheben.

Voraussetzungen

- Stellen Sie sicher, dass Sie über die Root-Benutzer-Anmeldedaten verfügen, um sich bei der virtuellen vRealize Log Insight-Appliance anzumelden.

- Wenn Sie eine Verbindung zu einer virtuellen vRealize Log Insight-Appliance unter Verwendung von SSH herstellen möchten, stellen Sie sicher, dass TCP-Port 22 geöffnet ist.

Vorgehensweise

1 Stellen Sie eine SSH-Verbindung zur vRealize Log Insight-vApp her und melden Sie sich als Root-Benutzer an.

2 Kopieren Sie das SSL-Zertifikat für den SMTP-Server in die vRealize Log Insight vApp.

3 Führen Sie den folgenden Befehl aus.

```
`/usr/java/latest/bin/keytool –import –alias zertifikat_name –file pfad_zum_zertifikat –keystore /usr/java/latest/lib/security/cacerts`
```

Hinweis Die äußeren Anführungszeichen werden mit dem Gravis-Zeichen eingegeben, das sich auf Ihrer Tastatur auf derselben Taste befindet wie die Tilde. Verwenden Sie keine einfachen Anführungszeichen.

4 Geben Sie das Standardkennwort **changeit** ein.

5 Führen Sie den Befehl `service loginsight restart` aus.

Weiter

Gehen Sie auf **Verwaltung > Smtp** und testen Sie über **Test-E-Mail senden** Ihre Einstellungen. Siehe „Konfigurieren des SMTP-Servers für vRealize Log Insight“, auf Seite 29.

Fehlschlagen des Upgrades, weil die Signatur der PAK-Datei nicht validiert werden kann

vRealize Log Insight-Upgrade schlägt aufgrund einer beschädigten PAK-Datei, einer abgelaufenen Lizenz oder nicht ausreichenden Festplattenspeichers fehl.

Problem

Das Upgrade von vRealize Log Insight schlägt fehl und die Fehlermeldung `Upgrade fehlgeschlagen. Fehler beim Upgrade: Signatur der PAK–Datei kann nicht validiert werden` wird angezeigt.

Ursache

Dieser Fehler kann die folgenden Ursachen haben:

- Bei der hochgeladenen Datei handelt es sich nicht um eine PAK-Datei.
- Die hochgeladene PAK-Datei ist nicht vollständig.
- Die Lizenz von vRealize Log Insight ist abgelaufen.
- Auf dem Root-Dateisystem der virtuellen vRealize Log Insight-Appliance ist nicht genügend Festplattenspeicher verfügbar.

Lösung

- Stellen Sie sicher, dass Sie eine PAK-Datei hochladen.
- Gleichen Sie „md5sum“ der PAK-Datei mit der VMware-Downloadsite ab.
- Stellen Sie sicher, dass mindestens eine gültige Lizenz für vRealize Log Insight konfiguriert ist.
- Melden Sie sich bei der virtuellen vRealize Log Insight-Appliance an und führen Sie `df –h` aus, um den verfügbaren Festplattenspeicher zu ermitteln.

Hinweis Legen Sie keine Dateien im Root-Dateisystem der virtuellen vRealize Log Insight-Appliance ab.

Fehlschlagen des Upgrades mit einem internen Serverfehler

Aufgrund eines Verbindungsproblems schlägt das vRealize Log Insight-Upgrade mit einem internen Serverfehler fehl.

Problem

Das Upgrade von vRealize Log Insight schlägt fehl und die Fehlermeldung `Upgrade fehlgeschlagen. Interner Serverfehler` wird angezeigt.

Ursache

Es ist ein Verbindungsproblem zwischen dem Client und dem Server aufgetreten. Dies geschieht beispielsweise, wenn Sie versuchen, ein Upgrade von einem Client auszuführen, welcher sich in einem WAN befindet.

Lösung

- Führen Sie das LI-Upgrade von einem Client in demselben LAN wie der Server aus.

Index

A

Abmeldung aller Benutzer **42**
Active Directory
  Benutzer **61**
  Gruppen **62**
Active Directory-Anmeldedaten **108**
Active Directory-Integration mit vROPs **81**
AD
  Authentifizierung **66**
  Benutzer **61**
  Gruppen **62**
  SSL **66, 67**
  TCL **66**
Adapter **82**
adding disks **18**
Admin-Kennwort **106**
Agenten
  Gruppe bearbeiten **55**
  Gruppe erstellen **55**
  Gruppe löschen **56**
  Gruppen **54**
  Inhaltspaket-Agentengruppe **56**
Agenten überwachen **53**
Agentengruppe bearbeiten **55**
Agentengruppe erstellen **55**
Agentengruppe löschen **56**
Agentengruppen
  arbeiten mit **54**
  bearbeiten **55**
  erstellen **55**
  Inhaltspaketgruppe hinzufügen **56**
  Löschen **56**
aktualisieren
  Befehlszeilenschnittstelle **12**
  über Benutzeroberfläche **13**
Anmeldung nicht möglich **108**
API **35**
Arbeitsspeicher hinzufügen **43**
Archiv exportieren, Archiv nach JSON exportieren, Archiv in Textdatei exportieren **39**
Aufgaben **74**
Ausschalten **43**

B

Benachrichtigungen, Log Insight **80**
Benachrichtigungsereignisse **71, 80**
Benutzeranmeldungen **60**
benutzerdefinierte Zertifikate **30**
benutzerdefiniertes SSL-Zertifikat, Hochladen **34**
Benutzerkonten
  löschen **65**
  Neu **60**
Benutzeroberflächen-Upgrade **13**
Benutzerrolle ändern **65**
Benutzerrolle erstellen **65**
Benutzerrollen **65**
Benutzerzugriff auf bestimmte Daten **64**
Berechtigungen **60**
Bereitstellung **46**
Bereitstellung der Appliance **46**
Bereitstellung der virtuellen Appliance **46**
Best Practices für das Sichern **91**

C

Cluster beitreten **48**
Clustermodus **48**
CPU hinzufügen **43**

D

Datenarchivierung **20**
Datensatz **64**
domain groups **62**
Domänenkonto **61**

E

E-Mail-Systemwarnungen **29**
Empfehlungen für Sicherungsvorgänge **93**
Ereignisse **74**
Ereignisweiterleitung, Ereignisweiterleitung konfigurieren, Ereignisse weiterleiten **40, 42**
Erzwungene Abmeldung **42**
ESXi konfigurieren **75**
ESXi-Konfiguration **75**

F

Fehlerbehebung, ESXi-Protokolle **103**
Fehlerbehebung für SMTP **108**
Fehlerbehebung für STARTTLS **108**

G

Glossar **7**
Grenzwerte für die Konfiguration **16**

H

Hinzufügen einer Suchdomäne **81**
Horizontalskalierungs-Warnungen **26**
Hostliste **70**
Hostübersicht **70**
Hostüberwachung **70**

I

Inhaltspaket **83**
Installation **46**
Integration
  vCenter Server **72**
  vRealize Operations Manager **79**
  vSphere **72**
Integration von Log Insight **71**
integrierter Lastausgleichsdienst **50**
interner Serverfehler **110**
IP-Adresse
  Ändern **17**
  Konfiguration **17**
IP-Adresseinstellungen **17**

K

Kennwort
  Admin **106**
  root **106**
Knoten aktualisieren **11**
Knoten entfernen **49**
Kontextbezogenen Start deaktivieren **88**

L

Lastausgleich **75**
Lastausgleichsdienst für die Erfassung **50**
LDAP SSL **67**
Linux-Agent **36**
Lizenzierung **18**
Log Insight
  Als Syslog-Server ausführen **74**
    Upgrade über Benutzeroberfläche, Upgrade auf Cluster **13**
Log Insight Linux Agent **35**
Log Insight Windows Agent **35**
Log Insight-Adapter **82, 88**
Log Insight-Agenten **36**
Log Insight-Archivformat **38**
Log Insight-Benachrichtigungen **80**
Log Insight-Cluster, Worker-Knoten hinzufügen **45**

M

Master-Knoten **48**

N

Neustart wird durchgeführt **42**
NFS **20**

P

PAK-Dateifehler **109**
PEM-Datei, erstellen **33**
Protokolldateien **105**
Protokolle importieren **39**
Protokollierungsdaten deaktivieren **44**
Protokollierungsdaten, Versenden einstellen **44**
Protokollimport **39**
Protokollrichtlinien **18**
Protokollweiterleitung
  ESXi **75**
  ESXi-Syslog **76**
  syslog **77**
  vCenter Server Appliance **78**

R

Richtlinien für das Sichern und Replizieren **93**
Richtlinien für das Sichern und Wiederherstellen **92**
Richtlinien für die Wiederherstellung und die Notfallwiederherstellung **95**
Richtlinien für Konfigurationsänderungen nach der Wiederherstellung **96**
Rollen **60**
Rollenbasierte Zugriffssteuerung **59, 60, 64**
Root-Kennwort **16, 106**
Root-SSH **16**
rotes Zeichen in der Symbolleiste **107**

S

Service, Neustart wird durchgeführt **42**
sichere Verbindung **35**
Sicherheitsmodell **59**
Sicherheitsrichtlinie **59**
signiertes Zertifikat, Hochladen **34**
SMTP **29**
SSH-Kennwort **16**
SSH-Root **16**
SSL **42, 67**
ssl certificates **30**
SSL-Funktionen **35**
SSL-Konfiguration **36**
SSL-Parameter **36**
SSL-Verbindung erzwingen **35**
SSL-Verbindung konfigurieren **35**

SSL-Zertifikat für STARTTLS **108**
Standard-Zeitlimit **38**
Start, kontextbezogen
  Aktivieren **84**
  deaktivieren **87**
Status **69**
storage increasing **18**
Support-Paket **105**
syslog **74**
Syslog-Konfiguration **75**
Systembenachrichtigung **21**
Systembenachrichtigungen **22, 26**
Systemprotokolle **105**
Systemwarnungen **29**
Systemzustand **69**
Systemzustand der virtuellen Appliance **69**

U

Uhrzeitsynchronisierung **28**
Unterstützte Upgrades **9**
upgrade cluster **10, 11**
Upgrade mit Befehlszeilenschnittstelle **12**
upgrade paths **9**
Upgrade schlägt fehl **109, 110**
upgrade worker **11**

V

vCenter Server
  Aufgaben **74**
  Ereignisse **74**
  Warnungen **74**
vCenter Server Appliance **78**
vCOps-Integration **81**
Versenden von Warnungen nicht möglich **107**
vRealize Operations Manager **71, 83**
vRealize Operations Manager-Inhaltspaket **83**
vSphere-Integration **72**

W

Warnungen **74**
Wiederherstellen auf einem anderen Host **97**
Windows-Agent **36**
Worker entfernen **49**
Worker-Knoten **48**
Worker-Knoten, hinzufügen zu einem Cluster **45**

Z

Zeitlimit deaktivieren **38**
Zeitlimit der Sitzung **38**
Zeitlimit, deaktivieren **38**
Zeitüberschreitung, ändern **38**
Zertifikatsdatei, combine **33**
Zertifikatssignierungs-Anforderung, Generieren **32**
Zertifizierungsanforderung an eine Zertifizierungsstelle **33**
Zielgruppe **7**
zu wenig Festplattenspeicher **104**
zu wenig Speicherplatz **104**